(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－252607
（P2002－252607A）
(43)公開日　平成14年９月６日(2002.9.6)

(51)Int.Cl.⁷		識別記号	FI		テーマコード(参考)	
Ｈ０４Ｌ	9/08		Ｇ０６Ｆ	15/00	３３０Ｚ	５Ｂ０８５
Ｇ０６Ｆ	15/00	３３０	Ｈ０４Ｌ	12/22		５Ｊ１０４
Ｈ０４Ｌ	12/22			12/56	２６０Ａ	５Ｋ０３０
	12/56	２６０		9/00	６０１Ｂ	

審査請求　未請求　請求項の数49　ＯＬ　（全 27 頁）

(21)出願番号　特願2001－31338(P2001－31338)

(22)出願日　平成13年２月７日(2001.2.7)

(31)優先権主張番号　特願2000－390926(P2000－390926)
(32)優先日　平成12年12月22日(2000.12.22)
(33)優先権主張国　日本（ＪＰ）

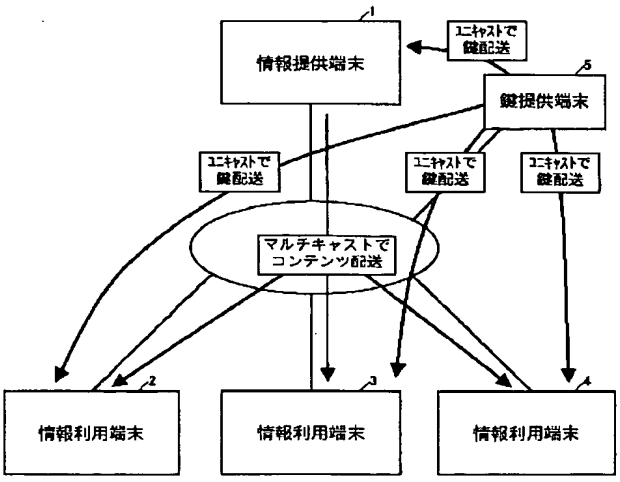
(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　庵　祥子
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　三宅　延久
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(74)代理人　100083552
弁理士　秋田　収喜

最終頁に続く

(54)【発明の名称】　情報配送方法及びその実施装置並びにその処理プログラムと記録媒体

(57)【要約】
【課題】　マルチキャストで配送されるコンテンツに対して、利用者の入れ替わりに対応した利用制御を行うことが可能な技術を提供する。
【解決手段】　コンテンツを暗号化または復号化する為の鍵をユニキャストで各情報利用端末に配送するステップと、前記ユニキャストで配送された鍵を情報利用端末で取得するステップと、前記取得した鍵を当該情報利用端末に保存するステップと、情報提供端末に保存した鍵によりコンテンツを暗号化するステップと、前記暗号化したコンテンツである暗号化コンテンツをマルチキャストで各情報利用端末に配送するステップと、前記マルチキャストで配送された暗号化コンテンツを情報利用端末で取得するステップと、前記取得した暗号化コンテンツを当該情報利用端末に保存した鍵で復号化するステップと、前記復号化したコンテンツを再生するステップとを有するものである。

図１



1

【特許請求の範囲】

【請求項１】　コンテンツをマルチキャストで情報提供端末から情報利用端末に配送する情報配送方法において、

コンテンツを暗号化または復号化する為の鍵を鍵提供端末で生成するステップと、前記生成した鍵をユニキャストで情報提供端末及び各情報利用端末に配送するステップと、前記ユニキャストで配送された鍵を情報提供端末で取得するステップと、前記取得した鍵を当該情報提供端末に保存するステップと、前記ユニキャストで配送された鍵を情報利用端末で取得するステップと、前記取得した鍵を当該情報利用端末に保存するステップと、

前記情報提供端末に保存した鍵によりコンテンツを暗号化するステップと、前記暗号化したコンテンツである暗号化コンテンツをマルチキャストで各情報利用端末に配送するステップと、前記マルチキャストで配送された暗号化コンテンツを情報利用端末で取得するステップと、前記取得した暗号化コンテンツを当該情報利用端末に保存した鍵で復号化するステップと、前記復号化したコンテンツを再生するステップとを有することを特徴とする情報配送方法。

【請求項２】　前記生成した鍵にそれらの鍵を識別する為の識別情報を付加するステップと、鍵の配送完了を示す鍵配送完了通知を受けて次の暗号化処理で使用する鍵の識別情報を指定するステップと、前記指定された識別情報を持つ鍵を用いてコンテンツを暗号化するステップと、

前記取得した暗号化コンテンツの暗号化で用いられた鍵の識別情報を確認するステップと、前記確認された識別情報に対応する鍵で暗号化コンテンツを復号化するステップとを有することを特徴とする請求項１に記載された情報配送方法。

【請求項３】　新規の鍵の取得を促す鍵更新広報をマルチキャストで各情報利用端末に送信するステップと、前記マルチキャストで送信された鍵更新広報を取得し、新規の鍵の配送を要求するステップとを有することを特徴とする請求項１または請求項２のいずれかに記載された情報配送方法。

【請求項４】　鍵の配送の際にＩＰｓｅｃの機能を利用することを特徴とする請求項１乃至請求項３のいずれか１項に記載された情報配送方法。

【請求項５】　コンテンツの利用資格を持つ利用者を示す配送先リストへの加入要求を情報利用端末から送信するステップと、前記送信された加入要求を受付けるステップと、前記加入要求の受付が行われた利用者の情報利用端末に対して暗号化コンテンツを復号化する為の鍵を配送するステップとを有することを特徴とする請求項１乃至請求項４のいずれか１項に記載された情報配送方法。

【請求項６】　前記加入要求を送信した利用者の利用資格が発生する日時を示す加入日時をデータベースに格納するステップと、現在の日時と前記データベースに格納した加入日時との差が所定の時間以内であるかまたは現在の日時が前記加入日時を経過している場合に、当該加入日時に対応する利用者の情報利用端末に暗号化コンテンツを復号化する為の鍵を配送するステップとを有することを特徴とする請求項５に記載された情報配送方法。

【請求項７】　前記送信された加入要求が受付けられたことを示す加入要求応答を、当該加入要求を送信した情報利用端末へ通知するステップを有することを特徴とする請求項５または請求項６のいずれかに記載された情報配送方法。

【請求項８】　前記配送先リストからの脱退要求を情報利用端末から送信するステップと、前記送信された脱退要求を受付けるステップと、前記脱退要求の受付が行われた利用者の情報利用端末に対する前記鍵の配送を抑止するステップとを有することを特徴とする請求項１乃至請求項７のいずれか１項に記載された情報配送方法。

【請求項９】　前記脱退要求を送信した利用者の利用資格が抹消される日時を示す脱退日時をデータベースに格納するステップと、現在の日時が前記脱退日時を経過しているかまたは次配送の鍵が脱退日時以降のコンテンツに相当する鍵である場合に、当該脱退日時に対応する利用者の情報利用端末への前記鍵の配送を抑止するステップとを有することを特徴とする請求項８に記載された情報配送方法。

【請求項１０】　前記送信された脱退要求が受付けられたことを示す脱退要求応答を、当該脱退要求を送信した情報利用端末へ通知するステップを有することを特徴とする請求項８または請求項９のいずれかに記載された情報配送方法。

【請求項１１】　コンテンツを暗号化または復号化する為の鍵を提供する鍵提供端末において、

コンテンツを暗号化または復号化する為の鍵を生成する鍵生成部と、情報提供端末及び情報提供端末から配送されるコンテンツの利用資格を持つ利用者の情報利用端末に前記生成した鍵をユニキャストで配送する鍵配送部とを備えることを特徴とする鍵提供端末。

【請求項１２】　コンテンツをマルチキャストで情報利用端末に提供する情報提供端末において、

コンテンツを暗号化または復号化する為の鍵を生成する鍵生成部と、前記生成した鍵を保存する鍵保存部と、情報提供端末から配送されるコンテンツの利用資格を持つ利用者の情報利用端末に前記生成した鍵をユニキャストで配送する鍵配送部と、

前記保存した鍵によりコンテンツを暗号化するコンテンツ暗号化部と、前記暗号化したコンテンツである暗号化コンテンツをマルチキャストで各情報利用端末に配送するコンテンツ配送部とを備えることを特徴とする情報提供端末。

【請求項１３】　前記生成した鍵にそれらの鍵を識別する為の識別情報を付加する識別情報付加部と、前記鍵配送部から鍵の配送完了を示す鍵配送完了通知を受けて次の暗号化処理で使用する鍵の識別情報を指定する鍵更新部とを備えることを特徴とする請求項１１または請求項１２のいずれかに記載された端末装置。

【請求項１４】　新規の鍵の取得を促す鍵更新広報をマルチキャストで各情報利用端末に送信する鍵更新広報部を備えることを特徴とする請求項１１乃至請求項１３のいずれか１項に記載された端末装置。

【請求項１５】　鍵の配送の際にＩＰｓｅｃの機能を利用することを特徴とする請求項１１乃至請求項１４のいずれか１項に記載された端末装置。

【請求項１６】　コンテンツの利用資格を持つ利用者を示す配送先リストへの加入要求を情報利用端末から受付ける加入要求受付部を備え、前記鍵配送部は、前記加入要求の受付が行われた利用者の情報利用端末に対して暗号化コンテンツを復号化する為の鍵を配送するものであることを特徴とする請求項１１乃至請求項１５のいずれか１項に記載された端末装置。

【請求項１７】　前記加入要求を送信した利用者の利用資格が発生する日時を示す加入日時をデータベースに格納するデータベース部を備え、前記鍵配送部は、現在の日時と前記データベースに格納した加入日時との差が所定の時間以内であるかまたは現在の日時が前記加入日時を経過している場合に、当該加入日時に対応する利用者の情報利用端末に暗号化コンテンツを復号化する為の鍵を配送するものであることを特徴とする請求項１６に記載された端末装置。

【請求項１８】　前記送信された加入要求が受付けられたことを示す加入要求応答を、当該加入要求を送信した情報利用端末へ通知する加入要求応答部を備えることを特徴とする請求項１６または請求項１７のいずれかに記載された端末装置。

【請求項１９】　前記配送先リストからの脱退要求を情報利用端末から受付ける脱退要求受付部を備え、前記鍵配送部は、前記脱退要求の受付が行われた利用者の情報利用端末に対する前記鍵の配送を抑止するものであることを特徴とする請求項１１乃至請求項１８のいずれか１項に記載された端末装置。

【請求項２０】　前記データベース部は、前記脱退要求を送信した利用者の利用資格が抹消される日時を示す脱退日時をデータベースに格納し、前記鍵配送部は、現在の日時が前記脱退日時を経過しているかまたは次配送の鍵が脱退日時以降のコンテンツに相当する鍵である場合に、当該脱退日時に対応する利用者の情報利用端末への前記鍵の配送を抑止するものであることを特徴とする請求項１９に記載された端末装置。

【請求項２１】　前記送信された脱退要求が受付けられたことを示す脱退要求応答を、当該脱退要求を送信した

情報利用端末へ通知する脱退要求応答部を備えることを特徴とする請求項１９または請求項２０のいずれかに記載された端末装置。

【請求項２２】　コンテンツをマルチキャストで情報利用端末に提供する情報提供端末において、利用資格を持つ利用者の情報利用端末に配送されるコンテンツを暗号化する為の鍵を鍵提供端末からユニキャストで取得する鍵取得部と、前記取得した鍵を保存する鍵保存部と、前記保存した鍵によりコンテンツを暗号化するコンテンツ暗号化部と、前記暗号化したコンテンツである暗号化コンテンツをマルチキャストで各情報利用端末に配送するコンテンツ配送部とを備えることを特徴とする情報提供端末。

【請求項２３】　マルチキャストで情報提供端末から配送されたコンテンツを取得する情報利用端末において、利用資格を持つ利用者の情報利用端末に配送された暗号化コンテンツを復号化する為の鍵を鍵提供端末からユニキャストで取得する鍵取得部と、前記取得した鍵を保存する鍵保存部と、暗号化されたコンテンツである暗号化コンテンツを情報提供端末からマルチキャストで取得するコンテンツ取得部と、前記取得した暗号化コンテンツを前記保存した鍵で復号化するコンテンツ復号化部と、前記復号化したコンテンツを再生するコンテンツ再生部とを備えることを特徴とする情報利用端末。

【請求項２４】　前記取得した暗号化コンテンツの暗号化で用いられた鍵の識別情報を確認する識別情報確認部を備え、前記確認された識別情報に対応する鍵で暗号化コンテンツを復号化することを特徴とする請求項２３に記載された情報利用端末。

【請求項２５】　新規の鍵の取得を促す鍵更新広報を取得し、新規の鍵の配送を要求する鍵更新情報取得部を備えることを特徴とする請求項２３または請求項２４のいずれかに記載された情報利用端末。

【請求項２６】　コンテンツの利用資格を持つ利用者を示す配送先リストへの加入要求を送信する加入要求部を備えることを特徴とする請求項２３乃至請求項２５のいずれか１項に記載された情報利用端末。

【請求項２７】　前記送信した加入要求が受付けられたことを示す加入要求応答を受信する加入要求応答受付部を備えることを特徴とする請求項２６に記載された情報利用端末。

【請求項２８】　前記配送先リストからの脱退要求を送信する脱退要求部を備えることを特徴とする請求項２３乃至請求項２７のいずれか１項に記載された情報利用端末。

【請求項２９】　前記送信した脱退要求が受付けられたことを示す脱退要求応答を受信する脱退要求応答受付部を備えることを特徴とする請求項２８に記載された情報利用端末。

【請求項３０】　コンテンツを暗号化または復号化する為の鍵を提供する鍵提供端末としてコンピュータを機能させる為のプログラムにおいて、
コンテンツを暗号化または復号化する為の鍵を生成する鍵生成部と、情報提供端末及び情報提供端末から配送されるコンテンツの利用資格を持つ利用者の情報利用端末に前記生成した鍵をユニキャストで配送する鍵配送部としてコンピュータを機能させることを特徴とするプログラム。

【請求項３１】　コンテンツをマルチキャストで情報利用端末に提供する情報提供端末としてコンピュータを機能させる為のプログラムにおいて、
コンテンツを暗号化または復号化する為の鍵を生成する鍵生成部と、前記生成した鍵を保存する鍵保存部と、情報提供端末から配送されるコンテンツの利用資格を持つ利用者の情報利用端末に前記生成した鍵をユニキャストで配送する鍵配送部と、
前記保存した鍵によりコンテンツを暗号化するコンテンツ暗号化部と、前記暗号化したコンテンツである暗号化コンテンツをマルチキャストで各情報利用端末に配送するコンテンツ配送部としてコンピュータを機能させることを特徴とするプログラム。

【請求項３２】　前記生成した鍵にそれらの鍵を識別する為の識別情報を付加する識別情報付加部と、前記鍵配送部から鍵の配送完了を示す鍵配送完了通知を受けて次の暗号化処理で使用する鍵の識別情報を指定する鍵更新部としてコンピュータを機能させることを特徴とする請求項３０または請求項３１のいずれかに記載されたプログラム。

【請求項３３】　新規の鍵の取得を促す鍵更新広報をマルチキャストで各情報利用端末に送信する鍵更新広報部としてコンピュータを機能させることを特徴とする請求項３０乃至請求項３２のいずれか１項に記載されたプログラム。

【請求項３４】　鍵の配送の際にＩＰｓｅｃの機能を利用することを特徴とする請求項３０乃至請求項３３のいずれか１項に記載されたプログラム。

【請求項３５】　コンテンツの利用資格を持つ利用者を示す配送先リストへの加入要求を情報利用端末から受付ける加入要求受付部と、前記加入要求の受付が行われた利用者の情報利用端末に対して暗号化コンテンツを復号化する為の鍵を配送する鍵配送部としてコンピュータを機能させることを特徴とする請求項３０乃至請求項３４のいずれか１項に記載されたプログラム。

【請求項３６】　前記加入要求を送信した利用者の利用資格が発生する日時を示す加入日時をデータベースに格納するデータベース部と、現在の日時と前記データベースに格納した加入日時との差が所定の時間以内であるかまたは現在の日時が前記加入日時を経過している場合に、当該加入日時に対応する利用者の情報利用端末に暗号化コンテンツを復号化する為の鍵を配送する鍵配送部としてコンピュータを機能させることを特徴とする請求項３５に記載されたプログラム。

【請求項３７】　前記送信された加入要求が受付けられたことを示す加入要求応答を、当該加入要求を送信した情報利用端末へ通知する加入要求応答部としてコンピュータを機能させることを特徴とする請求項３５または請求項３６のいずれかに記載されたプログラム。

【請求項３８】　前記配送先リストからの脱退要求を情報利用端末から受付ける脱退要求受付部と、前記脱退要求の受付が行われた利用者の情報利用端末に対する前記鍵の配送を抑止する鍵配送部としてコンピュータを機能させることを特徴とする請求項３０乃至請求項３７のいずれか１項に記載されたプログラム。

【請求項３９】　前記データベース部は、前記脱退要求を送信した利用者の利用資格が抹消される日時を示す脱退日時をデータベースに格納し、前記鍵配送部は、現在の日時が前記脱退日時を経過しているかまたは次配送の鍵が脱退日時以降のコンテンツに相当する鍵である場合に、当該脱退日時に対応する利用者の情報利用端末への前記鍵の配送を抑止するものであることを特徴とする請求項３８に記載されたプログラム。

【請求項４０】　前記送信された脱退要求が受付けられたことを示す脱退要求応答を、当該脱退要求を送信した情報利用端末へ通知する脱退要求応答部としてコンピュータを機能させることを特徴とする請求項３８または請求項３９のいずれかに記載されたプログラム。

【請求項４１】　コンテンツをマルチキャストで情報利用端末に提供する情報提供端末としてコンピュータを機能させる為のプログラムにおいて、
利用資格を持つ利用者の情報利用端末に配送されるコンテンツを暗号化する為の鍵を鍵提供端末からユニキャストで取得する鍵取得部と、前記取得した鍵を保存する鍵保存部と、
前記保存した鍵によりコンテンツを暗号化するコンテンツ暗号化部と、前記暗号化したコンテンツである暗号化コンテンツをマルチキャストで各情報利用端末に配送するコンテンツ配送部としてコンピュータを機能させることを特徴とするプログラム。

【請求項４２】　マルチキャストで情報提供端末から配送されたコンテンツを取得する情報利用端末としてコンピュータを機能させる為のプログラムにおいて、
利用資格を持つ利用者の情報利用端末に配送された暗号化コンテンツを復号化する為の鍵を鍵提供端末からユニキャストで取得する鍵取得部と、前記取得した鍵を保存する鍵保存部と、
暗号化されたコンテンツである暗号化コンテンツを情報提供端末からマルチキャストで取得するコンテンツ取得部と、前記取得した暗号化コンテンツを前記保存した鍵で復号化するコンテンツ復号化部と、前記復号化したコ

ンテンツを再生するコンテンツ再生部としてコンピュータを機能させることを特徴とするプログラム。

【請求項４３】　前記取得した暗号化コンテンツの暗号化で用いられた鍵の識別情報を確認する識別情報確認部と、前記確認された識別情報に対応する鍵で暗号化コンテンツを復号化するコンテンツ復号化部としてコンピュータを機能させることを特徴とする請求項４２に記載されたプログラム。

【請求項４４】　新規の鍵の取得を促す鍵更新広報を取得し、新規の鍵の配送を要求する鍵更新情報取得部としてコンピュータを機能させることを特徴とする請求項４２または請求項４３のいずれかに記載されたプログラム。

【請求項４５】　コンテンツの利用資格を持つ利用者を示す配送先リストへの加入要求を送信する加入要求部としてコンピュータを機能させることを特徴とする請求項４２乃至請求項４４のいずれか１項に記載されたプログラム。

【請求項４６】　前記送信した加入要求が受付けられたことを示す加入要求応答を受信する加入要求応答受付部としてコンピュータを機能させることを特徴とする請求項４５に記載されたプログラム。

【請求項４７】　前記配送先リストからの脱退要求を送信する脱退要求部としてコンピュータを機能させることを特徴とする請求項４２乃至請求項４６のいずれか１項に記載されたプログラム。

【請求項４８】　前記送信した脱退要求が受付けられたことを示す脱退要求応答を受信する脱退要求応答受付部としてコンピュータを機能させることを特徴とする請求項４７に記載されたプログラム。

【請求項４９】　請求項３０乃至請求項４８のいずれか１項のプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はコンテンツをマルチキャストで配送する情報配送システムに関し、特にストリームコンテンツを暗号化した暗号化コンテンツをマルチキャストで配送し、ユニキャストで配送された復号鍵で復号化することにより情報の利用制御を可能とし、利用者の加入及び脱退に応じて復号鍵の配送先を管理する情報配送システムに適用して有効な技術に関するものである。

【０００２】

【従来の技術】従来、複数の利用者に対してストリームコンテンツ等の同一のコンテンツを提供する場合、マルチキャストを用いることにより効率良くコンテンツの配送を行うことができる。このマルチキャストを用いたコンテンツの配送では、利用者がマルチキャストアドレスを指定することにより、誰でも簡単にそのコンテンツを利用することができる。

【０００３】また前記マルチキャストを用いて、利用資格を有する特定の利用者向けにコンテンツを提供しようとする場合には、そのコンテンツを利用者のみが復号できる状態で（例えば利用者に予め配られている鍵を利用する等）暗号化し、その暗号化コンテンツをマルチキャストで配送するという手法がある。利用者は、マルチキャストアドレスを指定して受信した暗号化コンテンツを、予め配られている鍵で復号化することにより、そのコンテンツを利用することができる。

【０００４】

【発明が解決しようとする課題】前記従来技術でマルチキャストを用いて暗号化すること無くコンテンツの配送を行った場合、マルチキャストアドレスを指定すれば誰でも簡単にそのストリームコンテンツを利用できる為、利用資格を有する特定の利用者向けにコンテンツを提供しようとした場合、前記暗号化を用いないマルチキャストではコンテンツの不正利用が行われるという問題があった。

【０００５】またストリームコンテンツを暗号化した暗号化コンテンツをマルチキャストで配送した場合、盗聴によるストリームコンテンツの不正利用は防御しているが、利用者がコンテンツの利用資格を失っても復号化する手段を保持し続けることが可能な為、不正利用される恐れがあるという問題があった。

【０００６】本発明の目的は上記問題を解決し、利用者がコンテンツの利用資格を失っても復号化する手段を保持し続けることが可能であると言う従来の問題点を解決し、マルチキャストで配送されるコンテンツに対して、利用者の入れ替わりに対応した利用制御を行うことが可能な技術を提供することにある。

【０００７】

【課題を解決するための手段】本発明は、コンテンツをマルチキャストで情報提供端末から情報利用端末に配送する情報配送システムにおいて、マルチキャストで情報提供端末から各情報利用端末に配送された暗号化コンテンツを、ユニキャストで当該情報利用端末に配送された鍵によって復号化するものである。

【０００８】本発明は、ストリームコンテンツ等を暗号化した暗号化コンテンツに対応する鍵をユニキャストで利用資格を持つ利用者に配送して更新することによって、マルチキャストストリームコンテンツを安全に配送すると共に、利用者の利用資格の更新を可能にすることを主な特徴とする。

【０００９】本発明の情報提供端末では以下の様にストリームコンテンツ等のコンテンツの暗号化及び配送を行なう。まず鍵提供端末の鍵生成部は、ストリームコンテンツＣの暗号化または復号化に利用する暗号鍵Ｋを生成する。暗号鍵Ｋには鍵が一意に定まる様な識別情報ｉを予め与えておくものとし、生成した暗号鍵Ｋｉを鍵配送

部に送付する。

【００１０】鍵配送部は、送付された暗号鍵Ｋｉを、情報提供端末及び現在の利用資格保持者集合Ｇの各情報利用端末にユニキャストで配送する。情報提供端末及び利用資格保持者集合Ｇの各情報利用端末に暗号鍵Ｋｉの配送を終了したら、配送が終了したことを鍵配送部から鍵更新部に知らせ、鍵更新部はコンテンツ暗号化部に送信が終了した鍵を通知する。また鍵提供端末は所定の時間間隔が経過した場合等、所定の条件で次の鍵の生成して配送するものとしても良い。鍵の配送においては先にマルチキャストで鍵の更新を呼びかけ、各情報利用端末からユニキャストで鍵を取得しても構わないものとする。

【００１１】コンテンツ暗号化部は、鍵更新部から暗号鍵Ｋｉの配送終了通知を受け取ったら、次パケットから暗号鍵Ｋｉを利用して暗号化を行って暗号化コンテンツＫｉ（Ｃ）を生成し、暗号化に使った鍵の識別情報ｉを暗号化コンテンツＫｉ（Ｃ）に付加する。更に暗号化コンテンツＫｉ（Ｃ）をコンテンツ配送部に送付し、コンテンツ配送部は暗号化コンテンツＫｉ（Ｃ）をマルチキャストで送付する。

【００１２】情報利用端末では以下の様にコンテンツの復号化及び再生を行う。まず鍵取得部は、鍵提供端末からユニキャストで送付される暗号鍵Ｋｉを受け取る。或いはマルチキャストで鍵更新の情報を鍵提供端末から取得したら各情報利用端末からユニキャストで暗号鍵Ｋｉの取得を行なう。受け取った暗号鍵Ｋｉを鍵保存部により保存した後、コンテンツ取得部は、情報提供端末からマルチキャストで送付される暗号化コンテンツＫｉ（Ｃ）を受け取る。コンテンツ復号化部は、送付された暗号化コンテンツＫｉ（Ｃ）から鍵の識別情報ｉを取り出し、その識別情報ｉに合った暗号鍵Ｋｉを鍵保存部から取得し、この暗号鍵Ｋｉを利用してコンテンツの復号化を行なう。コンテンツ再生部は、復号化したコンテンツの再生を行なう。

【００１３】鍵提供端末が所定の条件で鍵を生成して更新していくことによって、コンテンツをマルチキャストで配送しても利用資格保持者以外がコンテンツを利用することは不可能になり、また利用資格を失った利用者が長時間に渡ってコンテンツを不正利用し続けることを防止することができる。

【００１４】また本発明の鍵提供端末では、復号鍵の生成・管理及び配送先リストの管理を行ない、鍵提供端末で復号鍵の利用者リスト即ち配送先リストを管理することにより、その時点での利用者のみマルチキャストストリームコンテンツの利用を可能にする。鍵提供端末は、利用者が配送先リストに加入を行なう加入処理と利用者が資格を失う或いは意図的に配送先リストから脱退する脱退処理を管理することにより、利用者の管理を行なう。

【００１５】加入処理において、鍵提供端末と情報利用端末間では以下の処理が行なわれる。情報利用端末は、加入要求部を通じて鍵提供端末の加入要求受付部に対して加入要求を送付する。また情報利用端末は、加入したいチャネルの情報（コンテンツの名称、コンテンツの識別情報、マルチキャストアドレス等）や加入日時情報等を鍵提供端末に送付するものとする。

【００１６】鍵提供端末は、情報利用端末から送信された加入日時情報等をデータベースに格納しておき、現在の日時と前記データベースに格納した加入日時との差が所定の時間以内であるかまたは現在の日時が前記加入日時を経過している場合に、当該加入日時に対応する利用者の情報利用端末に、要求されているコンテンツに対応する復号鍵をユニキャストで送付する。ここで、対象者に対し鍵配送の準備が整ったという情報を鍵更新広報部から送付し、この情報を取得した利用状態にある情報利用端末はユニキャストで鍵情報を鍵提供端末から取得しても良い。

【００１７】以降、該当コンテンツに対応する復号鍵が更新された場合、鍵提供端末はデータベース部のデータを参照し該当する情報利用端末に更新された復号鍵をユニキャストで送付する。

【００１８】脱退処理において、鍵提供端末と情報利用端末間では以下の処理が行なわれる。情報利用端末は、脱退要求部を通じて、鍵提供端末の脱退要求受付部に対して脱退要求を送付する。また情報利用端末は、脱退したいチャネルの情報や脱退日時情報等を鍵提供端末に送付する。

【００１９】鍵提供端末は、情報利用端末から送信された脱退日時情報等をデータベースに格納しておき、現在の日時が前記脱退日時を経過しているかまたは次配送の鍵が脱退日時以降のコンテンツに相当する鍵である場合に、当該脱退日時に対応する利用者の情報利用端末への、要求されているコンテンツに対応する復号鍵の送付を取り止める。

【００２０】所定時間毎に鍵を生成して更新していき、鍵提供端末を利用して利用者の加入と脱退を管理して復号鍵をユニキャストで配送することにより、マルチキャストで暗号化コンテンツを配送しても利用者以外にコンテンツを利用することは不可能になり、また利用資格を失った利用者が長期に渡ってコンテンツを不正利用し続けることを防止することができる。

【００２１】以上の様に本発明の情報配送システムによれば、マルチキャストで情報提供端末から各情報利用端末に配送された暗号化コンテンツを、ユニキャストで当該情報利用端末に配送された鍵によって復号化するので、利用者がコンテンツの利用資格を失っても復号化する手段を保持し続けることが可能であると言う従来の問題点を解決し、マルチキャストで配送されるコンテンツに対して、利用者の入れ替わりに対応した利用制御を行うことが可能である。

【００２２】
【発明の実施の形態】（実施形態１）以下に鍵をユニキャストで配送した後にストリームコンテンツをマルチキャストで配送する実施形態１の情報配送システムについて説明する。
【００２３】図１は本実施形態の情報配送システムの概略構成を示す図である。図１に示す様に本実施形態の情報配送システムは、情報提供端末１と、情報利用端末２～４と、鍵提供端末５とを有している。
【００２４】情報提供端末１は、ストリームコンテンツをマルチキャストで情報利用端末２～４に配送する装置である。情報利用端末２～４は、マルチキャストで情報提供端末１から配送されたストリームコンテンツを取得する装置である。鍵提供端末５は、ストリームコンテンツを暗号化または復号化する為の鍵をユニキャストで情報提供端末１及び情報利用端末２～４に配送する装置である。
【００２５】本実施形態において、情報提供端末１と情報利用端末２～４と鍵提供端末５は、それぞれインターネットに接続されており、ネットワーク上でマルチキャストとユニキャストの通信が可能であるものとする。本実施形態では、ストリームコンテンツをマルチキャストで情報利用端末２～４に配送する情報提供端末１と、そのストリームコンテンツを暗号化または復号化する為の鍵を配送する鍵提供端末５とが別装置であるものとして説明するが、両者を同一の装置で実現しても良い。
【００２６】図２は本実施形態の情報提供端末１の概略構成を示す図である。図２に示す様に本実施形態の情報提供端末１は、ＣＰＵ２０１と、メモリ２０２と、磁気ディスク装置２０３と、入力装置２０４と、出力装置２０５と、ＣＤ－ＲＯＭ装置２０６と、通信装置２０７とを有している。
【００２７】ＣＰＵ２０１は、情報提供端末１全体の動作を制御する装置である。メモリ２０２は、情報提供端末１全体の動作を制御する際にその為の各種処理プログラムやデータをロードする記憶装置である。磁気ディスク装置２０３は、前記各種処理プログラムやデータを格納しておく記憶装置である。
【００２８】入力装置２０４は、ストリームコンテンツをマルチキャストで各情報利用端末へ配送する為の各種入力を行う装置である。出力装置２０５は、ストリームコンテンツの配送に伴う各種出力を行う装置である。
【００２９】ＣＤ－ＲＯＭ装置２０６は、前記各種処理プログラムを記録したＣＤ－ＲＯＭの内容を読み出す装置である。通信装置２０７は、インターネットやイントラネット等のネットワークを介して各情報利用端末及び鍵提供端末５との通信を行う装置である。
【００３０】また情報提供端末１は、鍵取得部２１１と、鍵保存部２１２と、コンテンツ暗号化部２１３と、コンテンツ配送部２１４とを有している。
【００３１】鍵取得部２１１は、利用資格を持つ利用者の情報利用端末に配送されるコンテンツを暗号化する為の鍵を鍵提供端末５からユニキャストで取得する処理部である。鍵保存部２１２は、鍵取得部２１１によって取得された鍵をメモリ２０２または磁気ディスク装置２０３に保存する処理部である。
【００３２】コンテンツ暗号化部２１３は、鍵保存部２１２によってメモリ２０２または磁気ディスク装置２０３に保存された鍵によりコンテンツを暗号化する処理部である。コンテンツ配送部２１４は、コンテンツ暗号化部２１３によって暗号化されたコンテンツである暗号化コンテンツをマルチキャストで各情報利用端末に配送する処理部である。
【００３３】情報提供端末１を鍵取得部２１１、鍵保存部２１２、コンテンツ暗号化部２１３及びコンテンツ配送部２１４として機能させる為のプログラムは、ＣＤ－ＲＯＭ等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する記録媒体はＣＤ－ＲＯＭ以外の他の記録媒体でも良い。また前記プログラムを当該記録媒体から情報処理装置にインストールして使用しても良いし、ネットワークを通じて当該記録媒体にアクセスして前記プログラムを使用するものとしても良い。
【００３４】図３は本実施形態の情報利用端末２の概略構成を示す図である。図３に示す様に本実施形態の情報利用端末２は、ＣＰＵ３０１と、メモリ３０２と、磁気ディスク装置３０３と、入力装置３０４と、出力装置３０５と、ＣＤ－ＲＯＭ装置３０６と、通信装置３０７とを有している。
【００３５】ＣＰＵ３０１は、情報利用端末２全体の動作を制御する装置である。メモリ３０２は、情報利用端末２全体の動作を制御する際にその為の各種処理プログラムやデータをロードする記憶装置である。磁気ディスク装置３０３は、前記各種処理プログラムやデータを格納しておく記憶装置である。
【００３６】入力装置３０４は、マルチキャストで情報提供端末１から配送されたストリームコンテンツを取得する為の各種入力を行う装置である。出力装置３０５は、ストリームコンテンツの取得に伴う各種出力を行う装置である。
【００３７】ＣＤ－ＲＯＭ装置３０６は、前記各種処理プログラムを記録したＣＤ－ＲＯＭの内容を読み出す装置である。通信装置３０７は、インターネットやイントラネット等のネットワークを介して情報提供端末１及び鍵提供端末５との通信を行う装置である。
【００３８】また情報利用端末２は、鍵取得部３１１と、鍵保存部３１２と、コンテンツ取得部３１３と、コンテンツ復号化部３１４と、コンテンツ再生部３１５とを有している。
【００３９】鍵取得部３１１は、利用資格を持つ利用者

の情報利用端末に配送された暗号化コンテンツを復号化する為の鍵を鍵提供端末５からユニキャストで取得する処理部である。鍵保存部３１２は、鍵取得部３１１によって取得された鍵をメモリ３０２または磁気ディスク装置３０３に保存する処理部である。

【００４０】コンテンツ取得部３１３は、暗号化コンテンツを情報提供端末１からマルチキャストで取得する処理部である。コンテンツ復号化部３１４は、コンテンツ取得部３１３によって取得された暗号化コンテンツを、鍵保存部３１２によってメモリ３０２または磁気ディスク装置３０３に保存された鍵で復号化する処理部である。コンテンツ再生部３１５は、コンテンツ復号化部３１４によって復号化されたコンテンツを再生する処理部である。

【００４１】情報利用端末２を鍵取得部３１１、鍵保存部３１２、コンテンツ取得部３１３、コンテンツ復号化部３１４及びコンテンツ再生部３１５として機能させる為のプログラムは、ＣＤ－ＲＯＭ等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する記録媒体はＣＤ－ＲＯＭ以外の他の記録媒体でも良い。また前記プログラムを当該記録媒体から情報処理装置にインストールして使用しても良いし、ネットワークを通じて当該記録媒体にアクセスして前記プログラムを使用するものとしても良い。

【００４２】なお情報利用端末３及び４についても情報利用端末２の構成と同様であるものとする。

【００４３】図４は本実施形態の鍵提供端末５の概略構成を示す図である。図４に示す様に本実施形態の鍵提供端末５は、ＣＰＵ４０１と、メモリ４０２と、磁気ディスク装置４０３と、入力装置４０４と、出力装置４０５と、ＣＤ－ＲＯＭ装置４０６と、通信装置４０７とを有している。

【００４４】ＣＰＵ４０１は、鍵提供端末５全体の動作を制御する装置である。メモリ４０２は、鍵提供端末５全体の動作を制御する際にその為の各種処理プログラムやデータをロードする記憶装置である。磁気ディスク装置４０３は、前記各種処理プログラムやデータを格納しておく記憶装置である。

【００４５】入力装置４０４は、コンテンツを暗号化または復号化する為の鍵をユニキャストで情報提供端末１及び各情報利用端末へ配送する為の各種入力を行う装置である。出力装置４０５は、コンテンツを暗号化または復号化する為の鍵の配送に伴う各種出力を行う装置である。

【００４６】ＣＤ－ＲＯＭ装置４０６は、前記各種処理プログラムを記録したＣＤ－ＲＯＭの内容を読み出す装置である。通信装置４０７は、インターネットやイントラネット等のネットワークを介して情報提供端末１及び各情報利用端末との通信を行う装置である。

【００４７】また鍵提供端末５は、鍵生成部４１１と、鍵配送部４１２とを有している。

【００４８】鍵生成部４１１は、コンテンツを暗号化または復号化する為の鍵を生成する処理部である。鍵配送部４１２は、情報提供端末１及び情報提供端末１から配送されるコンテンツの利用資格を持つ利用者の情報利用端末に鍵生成部４１１によって生成された鍵をユニキャストで配送する処理部である。

【００４９】鍵提供端末５を鍵生成部４１１及び鍵配送部４１２として機能させる為のプログラムは、ＣＤ－ＲＯＭ等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する記録媒体はＣＤ－ＲＯＭ以外の他の記録媒体でも良い。また前記プログラムを当該記録媒体から情報処理装置にインストールして使用しても良いし、ネットワークを通じて当該記録媒体にアクセスして前記プログラムを使用するものとしても良い。

【００５０】なおコンテンツを暗号化または復号化する為の鍵の生成及び配送を階層化された複数の鍵提供端末５によって行い、処理負荷を分散させても良い。

【００５１】本実施形態の情報提供端末１では、配送対象のストリームコンテンツが保存されているか、或いはリアルタイムでストリームコンテンツが取得されるものとし、このストリームコンテンツを情報提供端末１から情報利用端末２～４に配送して再生する際の例について説明する。なおこの例ではコンテンツの暗号化に利用される暗号鍵は復号鍵を兼ねているものとするが、公開鍵暗号方式の様に暗号鍵と復号鍵とが異なるものとしても良く、暗号鍵と復号鍵とが異なるものとした場合には、情報提供端末１に暗号鍵を配送し、コンテンツの利用資格を持つ利用者の情報利用端末には復号鍵の配送を行うものとする。

【００５２】図５は本実施形態の鍵提供端末５の鍵配送処理の処理手順を示すフローチャートである。図５に示す様に鍵提供端末５の鍵生成部４１１は、ストリームコンテンツであるコンテンツＣを暗号化または復号化する為の暗号鍵Ｋを生成し、鍵配送部４１２は、情報提供端末１及び情報提供端末１から配送されるコンテンツの利用資格を持つ利用者の情報利用端末に前記生成された鍵をユニキャストで配送する処理を行う。

【００５３】図５のステップ５０１で鍵提供端末５の鍵生成部４１１は、コンテンツＣを暗号化する為の暗号鍵Ｋを生成して鍵配送部４１２へ渡す。ステップ５０２で鍵配送部４１２は、前記生成された暗号鍵Ｋをユニキャストで情報提供端末１へ配送する。ここで配送の際にＩＰｓｅｃ(IP security protocol)等を用いて通信路をセキュアな状態に保っても構わないものとする。

【００５４】ステップ５０３で鍵配送部４１２は、情報提供端末１の利用資格者ＤＢの内容を参照し、情報提供端末１から配送されるコンテンツＣの利用資格を持つ利

用者について、その情報利用端末のＩＰアドレスを読み出す。

【００５５】ステップ５０４では、前記読み出した情報利用端末のＩＰアドレスを宛先としたユニキャストによって暗号鍵Ｋを配送する。ここで配送の際にＩＰｓｅｃ等を用いて通信路をセキュアな状態に保っても構わないものとする。

【００５６】ステップ５０５では、前記利用資格を持つ全ての利用者の情報利用端末に暗号鍵Ｋを配送したかどうかを調べ、まだ配送を行っていない情報利用端末がある場合にはステップ５０３へ戻って暗号鍵Ｋの配送を続行し、利用資格を持つ全ての利用者の情報利用端末への配送を完了した場合には暗号鍵Ｋの配送処理を終了する。

【００５７】図６は本実施形態の情報提供端末１または各情報利用端末の鍵取得処理の処理手順を示すフローチャートである。図６に示す様に情報提供端末１の鍵取得部２１１は、鍵提供端末５からユニキャストで配送された暗号鍵Ｋを取得して、鍵保存部２１２によりその暗号鍵Ｋを保存する処理を行う。同様に各情報利用端末の鍵取得部３１１は、鍵提供端末５からユニキャストで配送された暗号鍵Ｋを取得して、鍵保存部３１２によりその暗号鍵Ｋを保存する処理を行う。

【００５８】図６のステップ６０１で情報提供端末１の鍵取得部２１１は、鍵提供端末５からユニキャストで暗号鍵Ｋを受信しているかどうかを調べ、暗号鍵Ｋを受信している場合にはステップ６０２へ進み、前記受信した暗号鍵Ｋを取得してこれを鍵保存部２１２に渡す。ステップ６０３で鍵保存部２１２は、前記取得した暗号鍵Ｋをメモリ３０２または磁気ディスク装置３０３に保存する。

【００５９】各情報利用端末の場合も同様に図６のステップ６０１で各情報利用端末の鍵取得部３１１は、鍵提供端末５からユニキャストで暗号鍵Ｋを受信しているかどうかを調べ、暗号鍵Ｋを受信している場合にはステップ６０２へ進み、前記受信した暗号鍵Ｋを取得してこれを鍵保存部３１２に渡す。ステップ６０３で鍵保存部３１２は、前記取得した暗号鍵Ｋをメモリ３０２または磁気ディスク装置３０３に保存する。ここで各情報利用端末が暗号鍵Ｋを磁気ディスク装置３０３に保存する場合には暗号鍵Ｋを暗号化して保存を行うものとする。

【００６０】図７は本実施形態の情報提供端末１のコンテンツ配送処理の処理手順を示すフローチャートである。図７に示す様に情報提供端末１のコンテンツ暗号化部２１３は、鍵保存部２１２によって保存された暗号鍵Ｋを用いてコンテンツＣを暗号化し、前記暗号化されたコンテンツである暗号化コンテンツＫ（Ｃ）をコンテンツ配送部２１４によりマルチキャストで各情報利用端末に配送する処理を行う。

【００６１】図７のステップ７０１で情報提供端末１のコンテンツ暗号化部２１３は、鍵保存部２１２によってメモリ２０２または磁気ディスク装置２０３に保存されていた暗号鍵Ｋを読み出す。ステップ７０２では、配送対象のコンテンツＣを所定の単位で読み出し、ステップ７０３では、前記読み出したコンテンツＣを暗号鍵Ｋで暗号化して暗号化コンテンツＫ（Ｃ）を生成し、コンテンツ配送部２１４に渡す。ここで暗号化の単位はネットワーク配送を行う為のパケットの大きさを単位としても構わないものとする。またコンテンツの暗号化の際にコンテンツのスクランブル処理やハッシュ処理を併用しても良い。

【００６２】ステップ７０４でコンテンツ配送部２１４は、前記生成された暗号化コンテンツＫ（Ｃ）をマルチキャストで情報利用端末２～４へ配送する。ステップ７０５では、配送対象のコンテンツＣについて全てのデータを情報利用端末２～４に配送したかどうかを調べ、まだ配送を行っていないデータがある場合にはステップ７０２へ戻ってコンテンツＣの配送を続行し、全データの配送を完了した場合にはコンテンツＣの配送処理を終了する。

【００６３】図８は本実施形態の各情報利用端末のコンテンツ利用処理の処理手順を示すフローチャートである。図８に示す様に各情報利用端末のコンテンツ取得部３１３は、暗号化コンテンツＫ（Ｃ）を情報提供端末１からマルチキャストで取得し、コンテンツ復号化部３１４は、前記取得した暗号化コンテンツＫ（Ｃ）を鍵保存部３１２によって保存されていた暗号鍵Ｋにより復号化し、前記復号化されたコンテンツＣをコンテンツ再生部３１５により再生する処理を行う。

【００６４】図８のステップ８０１で各情報利用端末のコンテンツ取得部３１３は、情報提供端末１からマルチキャストで暗号化コンテンツＫ（Ｃ）を受信しているかどうかを調べ、暗号化コンテンツＫ（Ｃ）を受信している場合にはステップ８０２へ進み、前記受信した暗号化コンテンツＫ（Ｃ）を取得してコンテンツ復号化部３１４に渡す。

【００６５】ステップ８０３でコンテンツ復号化部３１４は、暗号鍵Ｋのメモリ３０２または磁気ディスク装置３０３からの読込みが未実行であるかどうかを調べ、暗号鍵Ｋの読込みが未実行である場合にはステップ８０４へ進む。ステップ８０４では、鍵保存部３１２によってメモリ３０２または磁気ディスク装置３０３に保存されている暗号鍵Ｋを読み出す。

【００６６】ステップ８０５では、ステップ８０２で取得した暗号化コンテンツＫ（Ｃ）をステップ８０４で読み出した暗号鍵Ｋによって復号化してコンテンツＣを生成する。ステップ８０６でコンテンツ再生部３１５は、前記復号化によって得られたコンテンツＣを再生する。

【００６７】前記の様に本実施形態では、情報提供端末１から配送されるコンテンツＣの利用資格を持つ利用者

の情報利用端末へユニキャストで暗号鍵Ｋ（復号兼用）を配送した後、暗号化コンテンツＫ（Ｃ）をマルチキャストで各情報利用端末へ配送しているので、コンテンツの利用資格を失った利用者による不正利用を防止しつつマルチキャストを利用した効率的なコンテンツの提供を行うことができる。

【００６８】以上説明した様に本実施形態の情報配送システムによれば、マルチキャストで情報提供端末から各情報利用端末に配送された暗号化コンテンツを、ユニキャストで当該情報利用端末に配送された鍵によって復号化するので、利用者がコンテンツの利用資格を失っても復号化する手段を保持し続けることが可能であると言う従来の問題点を解決し、マルチキャストで配送されるコンテンツに対して、利用者の入れ替わりに対応した利用制御を行うことが可能である。

【００６９】（実施形態２）以下に鍵を鍵提供端末から各情報利用端末へ配布して鍵の更新を行った後にストリームコンテンツをマルチキャストで配送する実施形態２の情報配送システムについて説明する。

【００７０】図９は本実施形態の鍵提供端末５の概略構成を示す図である。図９に示す様に本実施形態の鍵提供端末５は、識別情報付加部９１１と、鍵更新部９１２とを有している。

【００７１】識別情報付加部９１１は、前記生成した鍵にそれらの鍵を識別する為の識別情報を付加する処理部である。鍵更新部９１２は、鍵配送部４１２から鍵の配送完了を示す鍵配送完了通知を受けて次の暗号化処理で使用する鍵の識別情報を情報提供端末１に指定する処理部である。

【００７２】鍵提供端末５を識別情報付加部９１１及び鍵更新部９１２として機能させる為のプログラムは、ＣＤ－ＲＯＭ等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する記録媒体はＣＤ－ＲＯＭ以外の他の記録媒体でも良い。また前記プログラムを当該記録媒体から情報処理装置にインストールして使用しても良いし、ネットワークを通じて当該記録媒体にアクセスして前記プログラムを使用するものとしても良い。

【００７３】本実施形態において、情報提供端末１は実施形態１と同様の構成であるものとし、情報提供端末１と情報利用端末２～４と鍵提供端末５は、実施形態１と同様にそれぞれインターネットに接続されており、ネットワーク上でマルチキャストとユニキャストの通信が可能であるものとする。本実施形態では、ストリームコンテンツをマルチキャストで情報利用端末２～４に配送する情報提供端末１と、そのストリームコンテンツを暗号化または復号化する為の鍵を配送する鍵提供端末５とが別装置であるものとして説明するが、両者を同一の装置で実現しても良い。

【００７４】図１０は本実施形態の情報利用端末２の概略構成を示す図である。図１０に示す様に本実施形態の情報利用端末２は識別情報確認部１０１１を有している。識別情報確認部１０１１は、前記取得した暗号化コンテンツの暗号化で用いられた鍵の識別情報を確認する処理部である。

【００７５】情報利用端末２を識別情報確認部１０１１として機能させる為のプログラムは、ＣＤ－ＲＯＭ等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する記録媒体はＣＤ－ＲＯＭ以外の他の記録媒体でも良い。また前記プログラムを当該記録媒体から情報処理装置にインストールして使用しても良いし、ネットワークを通じて当該記録媒体にアクセスして前記プログラムを使用するものとしても良い。

【００７６】なお情報利用端末３及び４についても情報利用端末２の構成と同様であるものとする。

【００７７】本実施形態の情報提供端末１には、配送対象のストリームコンテンツが保存されているか、或いはリアルタイムでストリームコンテンツが取得されるものとし、鍵提供端末５から情報提供端末１及び各情報利用端末に鍵を、また情報提供端末１から各情報利用端末に暗号化コンテンツを送付し、各情報利用端末で暗号化コンテンツを復号化して再生する際の例について説明する。なおこの例ではコンテンツの暗号化に利用される暗号鍵は復号鍵を兼ねており、その鍵は所定の時間間隔で更新されるものとする。なお利用資格変更に伴って鍵が更新されるものとしたり、公開鍵暗号方式の様に暗号鍵と復号鍵とが異なるものとしても良く、暗号鍵と復号鍵とが異なるものとした場合には、情報提供端末１に暗号鍵を配送し、コンテンツの利用資格を持つ利用者の情報利用端末には復号鍵の配送を行うものとする。

【００７８】図１１は本実施形態の鍵提供端末５の鍵配送処理の処理手順を示すフローチャートである。図１１に示す様に鍵提供端末５の鍵生成部４１１は、ストリームコンテンツであるコンテンツＣを暗号化または復号化する為の暗号鍵Ｋを生成し、前記生成された暗号鍵Ｋにその鍵を識別する為の識別情報ｉを識別情報付加部９１１により付加する。また鍵配送部４１２により情報提供端末１及び各情報利用端末にその暗号鍵Ｋｉをユニキャストで配送した後、次の暗号化処理で使用する鍵の識別情報ｉを鍵更新部９１２により情報提供端末１に指定する処理を行う。

【００７９】図１１のステップ１１０１で鍵提供端末５の鍵生成部４１１は、所定の時間が経過した場合や情報提供端末１の利用資格者ＤＢ中の利用資格が変更された場合等の暗号鍵Ｋを生成する条件が成立したかどうかを調べ、暗号鍵Ｋを生成する条件が成立した場合にはステップ１１０２へ進む。

【００８０】ステップ１１０２では、コンテンツＣを暗

号化する為の暗号鍵Ｋを生成する。暗号鍵Ｋとして通信時にＩＰｓｅｃで利用されているものを利用しても構わないものとする。

【００８１】ステップ１１０３で識別情報付加部９１１は、前記生成された暗号鍵Ｋに識別情報ｉを付加して鍵配送部４１２へ渡す。この識別情報はＩＰｓｅｃのＳＡ(Security Association)に含まれる情報を利用しても構わないものとする。

【００８２】ステップ１１０４で鍵配送部４１２は、前記生成された暗号鍵Ｋｉをユニキャストで情報提供端末１へ配送する。ここで配送の際にＩＰｓｅｃ等を用いて通信路をセキュアな状態に保っても構わないものとする。

【００８３】ステップ１１０５で鍵配送部４１２は、情報提供端末１の利用資格者ＤＢの内容を参照し、情報提供端末１から配送されるコンテンツＣの利用資格を持つ利用者について、その情報利用端末のＩＰアドレスを読み出す。

【００８４】ステップ１１０６では、前記読み出した情報利用端末のＩＰアドレスを宛先としたユニキャストによって暗号鍵Ｋｉを配送する。ここで配送の際にＩＰｓｅｃ等を用いて通信路をセキュアな状態に保っても構わないものとする。

【００８５】ステップ１１０７では、前記利用資格を持つ全ての利用者の情報利用端末に暗号鍵Ｋｉを配送したかどうかを調べ、まだ配送を行っていない情報利用端末がある場合にはステップ１１０５へ戻って暗号鍵Ｋｉの配送を続行し、利用資格を持つ全ての利用者の情報利用端末への配送を完了した場合にはステップ１１０８へ進む。ここで鍵の配送の完了とは、各情報利用端末と鍵提供端末５がユニキャストで鍵の通信を行って正常終了した場合の他に、情報利用端末２～４からの応答が無く、タイムアウトした場合を含んでいても構わないものとする。

【００８６】ステップ１１０８では、利用資格を持った全ての利用者に対する暗号鍵Ｋｉの配送が完了したことを示す鍵配送完了通知を鍵更新部９１２に伝え、ステップ１１０９で鍵更新部９１２は、配送が完了した暗号鍵Ｋｉを次の暗号化処理で使用する鍵として決定し、その暗号鍵Ｋｉの識別情報ｉ或いは暗号鍵Ｋｉそのものの情報を情報提供端末１のコンテンツ暗号化部２１３に通知してステップ１１０１へ戻る。

【００８７】図１２は本実施形態の情報提供端末１または各情報利用端末の鍵取得処理の処理手順を示すフローチャートである。図１２に示す様に情報提供端末１の鍵取得部２１１は、鍵提供端末５からユニキャストで配送された暗号鍵Ｋｉを取得して、鍵保存部２１２によりその暗号鍵Ｋｉを保存する処理を行う。同様に各情報利用端末の鍵取得部３１１は、鍵提供端末５からユニキャストで配送された暗号鍵Ｋｉを取得して、鍵保存部３１２によりその暗号鍵Ｋｉを保存する処理を行う。

【００８８】図１２のステップ１２０１で情報提供端末１の鍵取得部２１１は、鍵提供端末５からユニキャストで暗号鍵Ｋｉを受信しているかどうかを調べ、暗号鍵Ｋｉを受信している場合にはステップ１２０２へ進み、前記受信した暗号鍵Ｋｉを取得して鍵保存部２１２に渡す。

【００８９】ステップ１２０３で鍵保存部２１２は、鍵提供端末５の識別情報付加部９１１によって付加された識別情報ｉを暗号鍵Ｋｉから読み出し、ステップ１２０４では、ステップ１２０２で取得した暗号鍵Ｋｉをステップ１２０３で読み出した識別情報ｉ毎に分類してメモリ３０２または磁気ディスク装置３０３に保存する。

【００９０】各情報利用端末の場合も同様に図１２のステップ１２０１で各情報利用端末の鍵取得部３１１は、鍵提供端末５からユニキャストで暗号鍵Ｋｉを受信しているかどうかを調べ、暗号鍵Ｋｉを受信している場合にはステップ１２０２へ進み、前記受信した暗号鍵Ｋｉを取得して鍵保存部３１２に渡す。

【００９１】ステップ１２０３で鍵保存部３１２は、鍵提供端末５の識別情報付加部９１１によって付加された識別情報ｉを暗号鍵Ｋｉから読み出し、ステップ１２０４では、ステップ１２０２で取得した暗号鍵Ｋｉをステップ１２０３で読み出した識別情報ｉ毎に分類してメモリ３０２または磁気ディスク装置３０３に保存する。ここで各情報利用端末が暗号鍵Ｋｉを磁気ディスク装置３０３に保存する場合には暗号鍵Ｋiを暗号化して保存を行うものとする。

【００９２】図１３は本実施形態の情報提供端末１のコンテンツ配送処理の処理手順を示すフローチャートである。図１３に示す様に情報提供端末１のコンテンツ暗号化部２１３は、鍵保存部２１２によって保存された鍵の内、鍵提供端末５の鍵更新部９１２により指定された識別情報ｉの暗号鍵Ｋｉを用いてコンテンツＣを暗号化し、前記暗号化されたコンテンツである暗号化コンテンツＫｉ（Ｃ）をコンテンツ配送部２１４によりマルチキャストで各情報利用端末に配送する処理を行う。

【００９３】図１３のステップ１３０１で情報提供端末１のコンテンツ暗号化部２１３は、鍵保存部２１２によってメモリ２０２または磁気ディスク装置２０３に保存されていた鍵の内、鍵提供端末５の鍵更新部９１２により指定された識別情報ｉの暗号鍵Ｋｉを読み出す。

【００９４】ステップ１３０２では、配送対象のコンテンツＣを所定の単位で読み出し、ステップ１３０３では、ステップ１３０２で読み出したコンテンツＣのデータをステップ１３０１で読み出した暗号鍵Ｋｉで暗号化して暗号化コンテンツＫｉ（Ｃ）を生成し、コンテンツ配送部２１４に渡す。ここで暗号化の単位はネットワーク配送を行う為のパケットの大きさを単位としても構わないものとする。またコンテンツの暗号化の際にコンテ

ンツのスクランブル処理やハッシュ処理を併用しても良い。

【００９５】ステップ１３０４でコンテンツ配送部２１４は、前記生成された暗号化コンテンツＫｉ（Ｃ）のヘッダー等に暗号鍵Ｋｉの識別情報ｉを付加する。なおここでＩＰｓｅｃのヘッダーを利用しても構わないものとする。

【００９６】ステップ１３０５では、前記識別情報ｉの付加された暗号化コンテンツＫｉ（Ｃ）をマルチキャストで情報利用端末２～４へ配送する。ステップ１３０６では、配送対象のコンテンツＣについて全てのデータを情報利用端末２～４に配送したかどうかを調べ、まだ配送を行っていないデータがある場合にはステップ１３０２へ戻ってコンテンツＣの配送を続行し、全データの配送を完了した場合にはコンテンツＣの配送処理を終了する。

【００９７】図１４は本実施形態の各情報利用端末のコンテンツ利用処理の処理手順を示すフローチャートである。図１４に示す様に各情報利用端末のコンテンツ取得部３１３は、暗号化コンテンツＫｉ（Ｃ）を情報提供端末１からマルチキャストで取得し、前記取得した暗号化コンテンツＫｉ（Ｃ）の暗号化で用いられた暗号鍵Ｋｉの識別情報ｉを識別情報確認部１０１１により確認する。そしてコンテンツ復号化部３１４は、鍵保存部３１２によって保存されていた鍵の内、識別情報確認部１０１１により指定された識別情報ｉの暗号鍵Ｋｉを用いて暗号化コンテンツＫｉ（Ｃ）を復号化し、前記復号化されたコンテンツＣをコンテンツ再生部３１５により再生する処理を行う。

【００９８】図１４のステップ１４０１で各情報利用端末のコンテンツ取得部３１３は、情報提供端末１からマルチキャストで暗号化コンテンツＫｉ（Ｃ）を受信しているかどうかを調べ、暗号化コンテンツＫｉ（Ｃ）を受信している場合にはステップ１４０２へ進み、前記受信した暗号化コンテンツＫｉ（Ｃ）を取得して識別情報確認部１０１１に渡す。

【００９９】ステップ１４０３で識別情報確認部１０１１は、前記取得した暗号化コンテンツＫｉ（Ｃ）のヘッダー等を参照し、暗号化コンテンツＫｉ（Ｃ）に付加されている識別番号ｉを確認してコンテンツ復号化部３１４へ通知する。

【０１００】ステップ１４０４でコンテンツ復号化部３１４は、識別情報確認部１０１１から通知されたものと同一の識別番号ｉを持つ暗号鍵Ｋｉの読込みが未実行であるかどうかを調べ、暗号鍵Ｋｉの読込みが未実行である場合にはステップ１４０５へ進む。

【０１０１】ステップ１４０５では、鍵保存部３１２によってメモリ３０２または磁気ディスク装置３０３に保存されている鍵の内、識別情報確認部１０１１から通知されたものと同一の識別番号ｉを持つ暗号鍵Ｋｉを読み出す。

【０１０２】ステップ１４０６では、ステップ１４０２で取得した暗号化コンテンツＫｉ（Ｃ）をステップ１４０５で読み出した暗号鍵Ｋｉによって復号化してコンテンツＣを生成し、ステップ１４０７でコンテンツ再生部３１５は、前記復号化によって得られたコンテンツＣを再生してステップ１４０１へ戻る。

【０１０３】前記の様に本実施形態では、情報提供端末１から配送されるコンテンツＣの利用資格を持つ利用者の情報利用端末へユニキャストで暗号鍵Ｋｉ（復号兼用）を配送した後、識別情報ｉを付加した暗号化コンテンツＫｉ（Ｃ）をマルチキャストで各情報利用端末へ配送しているので、コンテンツの利用資格を失った利用者による不正利用を防止しつつマルチキャストを利用した効率的なコンテンツの提供を行うことができる。

【０１０４】以上説明した様に本実施形態の情報配送システムによれば、マルチキャストで情報提供端末から各情報利用端末に配送された暗号化コンテンツを、ユニキャストで当該情報利用端末に配送された鍵によって復号化するので、利用者がコンテンツの利用資格を失っても復号化する手段を保持し続けることが可能であると言う従来の問題点を解決し、マルチキャストで配送されるコンテンツに対して、利用者の入れ替わりに対応した利用制御を行うことが可能である。

【０１０５】（実施形態３）以下に鍵提供端末の鍵を各情報利用端末から取得して鍵の更新を行った後にストリームコンテンツをマルチキャストで配送する実施形態３の情報配送システムについて説明する。

【０１０６】図１５は本実施形態の鍵提供端末５の概略構成を示す図である。図１５に示す様に本実施形態の鍵提供端末５は鍵更新広報部１５１１を有している。鍵更新広報部１５１１は、新規の鍵の取得を促す鍵更新広報をマルチキャストで各情報利用端末に送信する処理部である。

【０１０７】鍵提供端末５を鍵更新広報部１５１１として機能させる為のプログラムは、ＣＤ－ＲＯＭ等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する記録媒体はＣＤ－ＲＯＭ以外の他の記録媒体でも良い。また前記プログラムを当該記録媒体から情報処理装置にインストールして使用しても良いし、ネットワークを通じて当該記録媒体にアクセスして前記プログラムを使用するものとしても良い。

【０１０８】本実施形態において、情報提供端末１は実施形態１と同様の構成であるものとし、情報提供端末１と情報利用端末２～４と鍵提供端末５は、実施形態１と同様にそれぞれインターネットに接続されており、ネットワーク上でマルチキャストとユニキャストの通信が可能であるものとする。本実施形態では、ストリームコンテンツをマルチキャストで情報利用端末２～４に配送す

る情報提供端末１と、そのストリームコンテンツを暗号化または復号化する為の鍵を配送する鍵提供端末５とが別装置であるものとして説明するが、両者を同一の装置で実現しても良い。

【０１０９】図１６は本実施形態の情報利用端末２の概略構成を示す図である。図１６に示す様に本実施形態の情報利用端末２は鍵更新情報取得部１６１１を有している。鍵更新情報取得部１６１１は、新規の鍵の取得を促す鍵更新広報を鍵提供端末５から取得し、新規の鍵の配送を鍵提供端末５に要求する処理部である。

【０１１０】情報利用端末２を鍵更新情報取得部１６１１として機能させる為のプログラムは、ＣＤ－ＲＯＭ等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する記録媒体はＣＤ－ＲＯＭ以外の他の記録媒体でも良い。また前記プログラムを当該記録媒体から情報処理装置にインストールして使用しても良いし、ネットワークを通じて当該記録媒体にアクセスして前記プログラムを使用するものとしても良い。

【０１１１】なお情報利用端末３及び４についても情報利用端末２の構成と同様であるものとする。

【０１１２】本実施形態の情報提供端末１には、配送対象のストリームコンテンツが保存されているか、或いはリアルタイムでストリームコンテンツが取得されるものとし、鍵提供端末５から情報提供端末１及び情報利用端末に鍵を、また情報提供端末１から各情報利用端末に暗号化コンテンツを送付し、各情報利用端末で暗号化コンテンツを復号化して再生する際の例について説明する。なおこの例ではコンテンツの暗号化に利用される暗号鍵は復号鍵を兼ねており、その鍵は所定の時間間隔で更新されるものとする。なお利用資格変更に伴って鍵が更新されるものとしたり、公開鍵暗号方式の様に暗号鍵と復号鍵とが異なるものとしても良く、暗号鍵と復号鍵とが異なるものとした場合には、情報提供端末１に暗号鍵を配送し、コンテンツの利用資格を持つ利用者の情報利用端末には復号鍵の配送を行うものとする。また更新の際は鍵提供端末５が呼びかけ、それに応じる形で情報利用端末２～４が鍵の更新を行なうものとする。

【０１１３】図１７は本実施形態の鍵提供端末５の鍵配送処理の処理手順を示すフローチャートである。図１７に示す様に鍵提供端末５では、ストリームコンテンツであるコンテンツＣを暗号化または復号化する為の暗号鍵Ｋｉを生成した後、鍵更新広報部１５１１により新規の暗号鍵Ｋｉの取得を促す鍵更新広報をマルチキャストで各情報利用端末に送信し、各情報利用端末からの接続を受付けてその暗号鍵Ｋｉをユニキャストで配送する処理を行う。

【０１１４】図１７のステップ１７０１で鍵提供端末５の鍵生成部４１１は、所定の時間が経過した場合や情報提供端末１の利用資格者ＤＢ中の利用資格が変更された場合等の暗号鍵Ｋを生成する条件が成立したかどうかを調べ、暗号鍵Ｋを生成する条件が成立した場合にはステップ１７０２へ進む。

【０１１５】ステップ１７０２では、コンテンツＣを暗号化する為の暗号鍵Ｋを生成する。暗号鍵Ｋとして通信時にＩＰｓｅｃで利用されているものを利用しても構わないものとする。

【０１１６】ステップ１７０３で識別情報付加部９１１は、前記生成された暗号鍵Ｋに識別情報ｉを付加して鍵配送部４１２へ渡す。この識別情報はＩＰｓｅｃのＳＡに含まれる情報を利用しても構わないものとする。

【０１１７】ステップ１７０４で鍵配送部４１２は、前記生成された暗号鍵Ｋｉをユニキャストで情報提供端末１へ配送する。ここで配送の際にＩＰｓｅｃ等を用いて通信路をセキュアな状態に保っても構わないものとする。

【０１１８】ステップ１７０５で鍵更新広報部１５１１は、各情報利用端末に向けて新規の暗号鍵Ｋｉの取得を促す鍵更新広報をマルチキャストにより送信する。この広報を受け取った各情報利用端末は、暗号鍵Ｋｉを取得する為に鍵提供端末５へユニキャストで接続する。

【０１１９】ステップ１７０６で鍵配送部４１２は、ユニキャストを用いた情報利用端末からの接続要求があるかどうかを調べ、情報利用端末からの接続要求がある場合にはステップ１７０７へ進む。

【０１２０】ステップ１７０７では、情報提供端末１の利用資格者ＤＢの内容を参照し、前記接続要求が、情報提供端末１から配送されるコンテンツＣの利用資格を持つ利用者の情報利用端末から送信されているかどうかを調べ、前記接続要求が利用資格を持つ利用者の情報利用端末から送信されている場合にはステップ１７０８へ進む。

【０１２１】ステップ１７０８では、前記接続要求を行った情報利用端末へユニキャストによって暗号鍵Ｋｉを配送する。ここで配送の際にＩＰｓｅｃ等を用いて通信路をセキュアな状態に保っても構わないものとする。

【０１２２】ステップ１７０９では、前記利用資格を持つ全ての利用者の情報利用端末に暗号鍵Ｋｉを配送したかどうかを調べ、まだ配送を行っていない情報利用端末がある場合にはステップ１７０６へ戻って他の情報利用端末からの接続要求を待ち、利用資格を持つ全ての利用者の情報利用端末への配送を完了した場合にはステップ１７１０へ進む。ここで鍵の配送の完了とは、各情報利用端末と鍵提供端末５がユニキャストで鍵の通信を行って正常終了した場合の他に、情報利用端末２～４からの応答が無く、タイムアウトした場合を含んでいても構わないものとする。また鍵提供端末５の鍵配送に対する応答を所定時間で区切り、その区切りをもって鍵配送完了通知としても構わないものとする。

【０１２３】ステップ１７１０では、利用資格を持った

全ての利用者に対する暗号鍵Ｋｉの配送が完了したことを示す鍵配送完了通知を鍵更新部９１２に伝え、ステップ１７１１で鍵更新部９１２は、配送が完了した暗号鍵Ｋｉを次の暗号化処理で使用する鍵として決定し、その暗号鍵Ｋｉの識別情報ｉ或いは暗号鍵Ｋｉそのものの情報を情報提供端末１のコンテンツ暗号化部２１３に通知してステップ１７０１へ戻る。

【０１２４】図１８は本実施形態の情報提供端末１または各情報利用端末の鍵取得処理の処理手順を示すフローチャートである。図１８に示す様に各情報利用端末は、鍵更新情報取得部１６１１により新規の暗号鍵Ｋｉの取得を促す鍵更新広報を鍵提供端末５から取得し、新規の暗号鍵Ｋｉの配送を鍵提供端末５に要求してユニキャストで配送された暗号鍵Ｋｉを取得する処理を行う。

【０１２５】図１８のステップ１８０１で各情報利用端末の鍵更新情報取得部１６１１は、鍵提供端末５からマルチキャストで新規の暗号鍵Ｋｉの取得を促す鍵更新広報を受信しているかどうかを調べ、鍵更新広報を受信している場合にはステップ１８０２へ進み、鍵提供端末５へユニキャストで接続して暗号鍵Ｋｉの配送を要求する。

【０１２６】ステップ１８０３で鍵取得部３１１は、鍵提供端末５からユニキャストで暗号鍵Ｋｉを受信しているかどうかを調べ、暗号鍵Ｋｉを受信している場合にはその暗号鍵Ｋｉを取得して鍵保存部３１２に渡す。

【０１２７】ステップ１８０４で鍵保存部３１２は、鍵提供端末５の識別情報付加部９１１によって付加された識別情報ｉを暗号鍵Ｋｉから読み出し、ステップ１８０４では、ステップ１８０２で取得した暗号鍵Ｋｉをステップ１８０３で読み出した識別情報ｉ毎に分類してメモリ３０２または磁気ディスク装置３０３に保存する。ここで磁気ディスク装置３０３に保存する場合には暗号鍵Ｋｉを暗号化して保存を行うものとする。

【０１２８】また本実施形態では、実施形態２と同様にしてコンテンツ配送処理を行う。すなわち、図１３に示す様に情報提供端末１のコンテンツ暗号化部２１３は、鍵保存部２１２によって保存された鍵の内、鍵提供端末５の鍵更新部９１２により指定された識別情報ｉの暗号鍵Ｋｉを用いてコンテンツＣを暗号化し、前記暗号化されたコンテンツである暗号化コンテンツＫｉ（Ｃ）をコンテンツ配送部２１４によりマルチキャストで各情報利用端末に配送する処理を行う。

【０１２９】また図１４に示す様に各情報利用端末のコンテンツ取得部３１３は、暗号化コンテンツＫｉ（Ｃ）を情報提供端末１からマルチキャストで取得し、前記取得した暗号化コンテンツＫｉ（Ｃ）の暗号化で用いられた暗号鍵Ｋｉの識別情報ｉを識別情報確認部１０１１により確認する。そしてコンテンツ復号化部３１４は、鍵保存部３１２によって保存されていた鍵の内、識別情報確認部１０１１により指定された識別情報ｉの暗号鍵Ｋｉを用いて暗号化コンテンツＫｉ（Ｃ）を復号化し、前記復号化されたコンテンツＣをコンテンツ再生部３１５により再生する処理を行う。

【０１３０】前記の様に本実施形態では、新規の暗号鍵Ｋｉの取得を促す鍵更新広報をマルチキャストで各情報利用端末に送信した後、情報提供端末１から配送されるコンテンツＣの利用資格を持つ利用者の情報利用端末へユニキャストで暗号鍵Ｋｉ（復号兼用）を配送した後、識別情報ｉを付加した暗号化コンテンツＫｉ（Ｃ）をマルチキャストで各情報利用端末へ配送しているので、コンテンツの利用資格を失った利用者による不正利用を防止しつつマルチキャストを利用した効率的なコンテンツの提供を行うことができる。

【０１３１】以上説明した様に本実施形態の情報配送システムによれば、マルチキャストで情報提供端末から各情報利用端末に配送された暗号化コンテンツを、ユニキャストで当該情報利用端末に配送された鍵によって復号化するので、利用者がコンテンツの利用資格を失っても復号化する手段を保持し続けることが可能であると言う従来の問題点を解決し、マルチキャストで配送されるコンテンツに対して、利用者の入れ替わりに対応した利用制御を行うことが可能である。

【０１３２】（実施形態４）以下に利用者の加入及び脱退に応じてコンテンツの復号鍵の配送先を管理し、復号鍵を鍵提供端末から各情報利用端末へ配布する実施形態４の情報配送システムについて説明する。

【０１３３】図１９は本実施形態の情報配送システムの概略構成を示す図である。本実施形態において、情報提供端末１と情報利用端末２～４と鍵提供端末５はそれぞれインターネットに接続されており、ネットワーク上でマルチキャストとユニキャストの通信が可能であるものとする。本実施形態では、ストリームコンテンツをマルチキャストで情報利用端末２～４に配送する情報提供端末１と、そのストリームコンテンツを暗号化または復号化する為の鍵を配送する鍵提供端末５とが別装置であるものとして説明するが、両者を同一の装置で実現しても良い。なお本実施形態では鍵提供端末５で鍵を生成するものとするが、情報提供端末１で鍵を生成するものとしても良い。

【０１３４】図２０は本実施形態の鍵提供端末５の概略構成を示す図である。図２０に示す様に本実施形態の鍵提供端末５は利用資格者ＤＢ２００８を有している。利用資格者ＤＢ２００８は、コンテンツの利用資格を持つ利用者を示す配送先リストの情報として、利用者の利用チャネル情報や加入日時及び脱退日時を格納するデータベースである。

【０１３５】また鍵提供端末５は、加入要求受付部２０１１と、データベース部２０１２と、脱退要求受付部２０１３とを有している。

【０１３６】加入要求受付部２０１１は、前記配送先リ

ストへの加入要求を情報利用端末２～４から受付ける処理部である。データベース部２０１２は、前記加入要求を送信した利用者の利用チャネルと利用者の利用資格が発生する日時を示す加入日時とを利用資格者ＤＢ２００８に格納する処理部である。脱退要求受付部２０１３は、前記配送先リストからの脱退要求を情報利用端末２～４から受付ける処理部である。

【０１３７】鍵提供端末５を加入要求受付部２０１１、データベース部２０１２及び脱退要求受付部２０１３として機能させる為のプログラムは、ＣＤ－ＲＯＭ等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する記録媒体はＣＤ－ＲＯＭ以外の他の記録媒体でも良い。また前記プログラムを当該記録媒体から情報処理装置にインストールして使用しても良いし、ネットワークを通じて当該記録媒体にアクセスして前記プログラムを使用するものとしても良い。

【０１３８】本実施形態において、鍵提供端末５のその他の構成は実施形態２と同様であるものとし、情報提供端末１は利用資格者ＤＢ２００８が鍵提供端末５にあることを除いて実施形態１と同様の構成であるものとする。

【０１３９】図２１は本実施形態の情報利用端末２の概略構成を示す図である。図２１に示す様に本実施形態の情報利用端末２は、加入要求部２１１１と、脱退要求部２１１２とを有している。

【０１４０】加入要求部２１１１は、前記配送先リストへの加入要求を鍵提供端末５に送信する処理部である。脱退要求部２１１２は、前記配送先リストからの脱退要求を鍵提供端末５に送信する処理部である。

【０１４１】情報利用端末２を加入要求部２１１１及び脱退要求部２１１２として機能させる為のプログラムは、ＣＤ－ＲＯＭ等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する記録媒体はＣＤ－ＲＯＭ以外の他の記録媒体でも良い。また前記プログラムを当該記録媒体から情報処理装置にインストールして使用しても良いし、ネットワークを通じて当該記録媒体にアクセスして前記プログラムを使用するものとしても良い。

【０１４２】本実施形態において、情報利用端末２のその他の構成は実施形態２と同様であるものとし、情報利用端末３及び４についても情報利用端末２の構成と同様であるものとする。

【０１４３】本実施形態の情報提供端末１には、配送対象のストリームコンテンツが保存されているか、或いはリアルタイムでストリームコンテンツが取得されるものとし、鍵提供端末５から情報提供端末１及び各情報利用端末に鍵を、また情報提供端末１から各情報利用端末に暗号化コンテンツを送付し、各情報利用端末で暗号化コンテンツを復号化して再生する際の例について説明する。なおこの例ではコンテンツの暗号化に利用される暗号鍵は復号鍵を兼ねており、その鍵は所定の時間間隔で更新されるものとする。なお利用資格変更に伴って鍵が更新されるものとしたり、公開鍵暗号方式の様に暗号鍵と復号鍵とが異なるものとしても良く、暗号鍵と復号鍵とが異なるものとした場合には、情報提供端末１に暗号鍵を配送し、コンテンツの利用資格を持つ利用者の情報利用端末には復号鍵の配送を行うものとする。

【０１４４】図２２は本実施形態の加入要求処理の処理手順を示すフローチャートである。図２２に示す様に各情報利用端末の加入要求部２１１１は、コンテンツの利用資格を持つ利用者を示す配送先リストへの加入要求を鍵提供端末５に送信する処理を行う。

【０１４５】ステップ２２０１で各情報利用端末の加入要求部２１１１は、コンテンツの利用資格を持つ利用者を示す配送先リストへの加入指示の利用者からの入力を受付けているかどうかを調べ、前記配送先リストへの加入指示を受付けている場合にはステップ２２０２へ進む。

【０１４６】ステップ２２０２では、当該情報利用端末を一意に指定できる情報として、情報利用端末の識別子、ＩＰアドレス、サービス加入時のユーザ情報または端末情報等を磁気ディスク装置３０３から読み出す。

【０１４７】ステップ２２０３では、利用者が加入したいチャネル情報として、コンテンツの名称、コンテンツ識別情報、マルチキャストアドレス等の情報と、当該コンテンツの利用を開始したい日時を示す加入日時の入力を受付ける。ここで当該コンテンツの利用可能な期間を示す加入期間や、当該コンテンツの利用を終了したい日時を示す脱退日時の入力を受付けても良い。また加入日時を省略しても構わないものとし、省略可能とする場合は省略時の加入日時は「即時」であるとする等予め規則を決めておくものとする。

【０１４８】ステップ２２０４では、前記読み出した当該情報利用端末を一意に指定できる情報及び前記受付けたチャネル情報と共に、前記配送先リストへの加入要求を鍵提供端末５に送信する。

【０１４９】図２３は本実施形態の加入要求受付処理の処理手順を示すフローチャートである。図２３に示す様に鍵提供端末５の加入要求受付部２０１１は、前記配送先リストへの加入要求を情報利用端末２～４から受付ける処理を行う。またデータベース部２０１２は、前記加入要求を送信した利用者の利用チャネルと利用者の利用資格が発生する日時を示す加入日時とを利用資格者ＤＢ２００８に格納する処理を行う。

【０１５０】ステップ２３０１で鍵提供端末５の加入要求受付部２０１１は、コンテンツの利用資格を持つ利用者を示す配送先リストへの加入要求と情報利用端末を一意に指定できる情報及びチャネル情報を情報利用端末２

～４から受信しているかどうかを調べ、前記配送先リストへの加入要求を受信している場合にはステップ２３０２へ進む。

【０１５１】ステップ２３０２でデータベース部２０１２は、前記加入要求と共に送信された、情報利用端末の識別子、ＩＰアドレス、サービス加入時のユーザ情報または端末情報等の情報利用端末を一意に指定できる情報や、コンテンツの名称、コンテンツ識別情報、マルチキャストアドレス等のチャネル情報、当該コンテンツの利用を開始したい日時を示す加入日時を利用資格者ＤＢ２００８に格納する。ここで当該コンテンツの利用可能な期間を示す加入期間や、当該コンテンツの利用を終了したい日時を示す脱退日時も送信されている場合には、脱退日時の格納も行う。また加入日時が省略されている場合には、予め決められている規則に従って加入日時を「即時」等に設定する。

【０１５２】図２４は本実施形態の脱退要求処理の処理手順を示すフローチャートである。図２４に示す様に各情報利用端末の脱退要求部２１１２は、前記配送先リストからの脱退要求を鍵提供端末５に送信する処理を行う。なお加入要求時に加入期間や脱退日時の入力を行っている場合にはこの脱退要求処理を省略することができる。

【０１５３】ステップ２４０１で各情報利用端末の脱退要求部２１１２は、コンテンツの利用資格を持つ利用者を示す配送先リストからの脱退指示の利用者からの入力を受付けているかどうかを調べ、前記配送先リストからの脱退指示を受付けている場合にはステップ２４０２へ進む。

【０１５４】ステップ２４０２では、当該情報利用端末を一意に指定できる情報として、情報利用端末の識別子、ＩＰアドレス、サービス脱退時のユーザ情報または端末情報等を磁気ディスク装置３０３から読み出す。

【０１５５】ステップ２４０３では、利用者が脱退したいチャネル情報として、コンテンツの名称、コンテンツ識別情報、マルチキャストアドレス等の情報と、当該コンテンツの利用を終了したい日時を示す脱退日時の入力を受付ける。ここで脱退日時を省略しても構わないものとし、省略可能とする場合は省略時の脱退日時は「即時」であるとする等予め規則を決めておくものとする。

【０１５６】ステップ２４０４では、前記読み出した当該情報利用端末を一意に指定できる情報及び前記受付けたチャネル情報と共に、前記配送先リストからの脱退要求を鍵提供端末５に送信する。

【０１５７】図２５は本実施形態の脱退要求受付処理の処理手順を示すフローチャートである。図２５に示す様に鍵提供端末５の脱退要求受付部２０１３は、前記配送先リストからの脱退要求を情報利用端末２～４から受付ける処理を行う。

【０１５８】ステップ２５０１で鍵提供端末５の脱退要求受付部２０１３は、コンテンツの利用資格を持つ利用者を示す配送先リストからの脱退要求と情報利用端末を一意に指定できる情報及びチャネル情報を情報利用端末２～４から受信しているかどうかを調べ、前記配送先リストへの脱退要求を受信している場合にはステップ２５０２へ進む。

【０１５９】ステップ２５０２でデータベース部２０１２は、前記脱退要求と共に送信された情報利用端末を一意に指定できる情報及びチャネル情報に該当するレコードを利用資格者ＤＢ２００８から検索し、前記チャネル情報中の脱退日時の情報を当該レコードに格納する。また脱退日時が省略されている場合には、予め決められている規則に従って脱退日時を「即時」等に設定する。

【０１６０】図２６は本実施形態の鍵提供端末５の鍵配送処理の処理手順を示すフローチャートである。図２６に示す様に鍵提供端末５の鍵生成部４１１は、ストリームコンテンツであるコンテンツＣを暗号化または復号化する為の暗号鍵Ｋを生成し、前記生成された暗号鍵Ｋにその鍵を識別する為の識別情報ｉを識別情報付加部９１１により付加する。また鍵配送部４１２により情報提供端末１及び各情報利用端末にその暗号鍵Ｋｉをユニキャストで配送した後、次の暗号化処理で使用する鍵の識別情報ｉを鍵更新部９１２により情報提供端末１に指定する処理を行う。

【０１６１】図２６のステップ２６０１で鍵提供端末５の鍵生成部４１１は、所定の時間が経過した場合や情報提供端末１の利用資格者ＤＢ２００８中の利用資格が変更された場合等の暗号鍵Ｋを生成する条件が成立したかどうかを調べ、暗号鍵Ｋを生成する条件が成立した場合にはステップ２６０２へ進む。

【０１６２】ステップ２６０２では、コンテンツＣを暗号化する為の暗号鍵Ｋを生成する。暗号鍵Ｋとして通信時にＩＰｓｅｃで利用されているものを利用しても構わないものとする。

【０１６３】ステップ２６０３で識別情報付加部９１１は、前記生成された暗号鍵Ｋに識別情報ｉを付加して鍵配送部４１２へ渡す。この識別情報はＩＰｓｅｃのＳＡに含まれる情報を利用しても構わないものとする。

【０１６４】ステップ２６０４で鍵配送部４１２は、前記生成された暗号鍵Ｋｉをユニキャストで情報提供端末１へ配送する。ここで配送の際にＩＰｓｅｃ等を用いて通信路をセキュアな状態に保っても構わないものとする。

【０１６５】ステップ２６０５で鍵配送部４１２は、情報提供端末１の利用資格者ＤＢ２００８の内容を参照し、情報提供端末１から配送されるコンテンツＣの名称がそのチャネル情報中に含まれているレコードの加入日時及び脱退日時を読み出す。

【０１６６】ステップ２６０６では、現在の日時と利用資格者ＤＢ２００８から前記読み出した加入日時とを比

較し、それらの差が所定の時間以内であるかまたは現在の日時が前記加入日時を経過している場合にはステップ２６０７へ進む。

【０１６７】ステップ２６０７では、現在の日時と利用資格者ＤＢ２００８から前記読み出した脱退日時とを比較し、現在の日時が前記脱退日時を経過しておらず、配送対象の鍵が脱退日時以前に配送されるコンテンツの鍵である場合にはステップ２６０８へ進む。

【０１６８】ステップ２６０８では、前記レコードから、その情報利用端末のＩＰアドレスを読み出し、そのＩＰアドレスを宛先としたユニキャストによって暗号鍵Ｋｉを配送する。ここで配送の際にＩＰｓｅｃ等を用いて通信路をセキュアな状態に保っても構わないものとする。

【０１６９】ステップ２６０９では、前記利用資格を持つ全ての利用者の情報利用端末に暗号鍵Ｋｉを配送したかどうかを調べ、まだ配送を行っていない情報利用端末がある場合にはステップ２６０５へ戻って暗号鍵Ｋｉの配送を続行し、利用資格を持つ全ての利用者の情報利用端末への配送を完了した場合にはステップ２６１０へ進む。ここで鍵の配送の完了とは、各情報利用端末と鍵提供端末５がユニキャストで鍵の通信を行って正常終了した場合の他に、情報利用端末２～４からの応答が無く、タイムアウトした場合を含んでいても構わないものとする。

【０１７０】ステップ２６１０では、利用資格を持った全ての利用者に対する暗号鍵Ｋｉの配送が完了したことを示す鍵配送完了通知を鍵更新部９１２に伝え、ステップ２６１１で鍵更新部９１２は、配送が完了した暗号鍵Ｋｉを次の暗号化処理で使用する鍵として決定し、その暗号鍵Ｋｉの識別情報ｉ或いは暗号鍵Ｋｉそのものの情報を情報提供端末１のコンテンツ暗号化部２１３に通知してステップ２６０１へ戻る。

【０１７１】次に本実施形態の情報利用端末２～４では、実施形態２と同様にして暗号鍵Ｋｉを取得する。すなわち図１２に示す様に情報利用端末２～４の鍵取得部３１１は、鍵提供端末５からユニキャストで暗号鍵Ｋｉを受信して鍵保存部３１２に渡し、鍵保存部３１２は、鍵提供端末５の識別情報付加部９１１によって付加された識別情報ｉを暗号鍵Ｋｉから読み出し、暗号鍵Ｋｉを識別情報ｉ毎に分類してメモリ３０２または磁気ディスク装置３０３に保存する。ここで各情報利用端末が暗号鍵Ｋｉを磁気ディスク装置３０３に保存する場合には暗号鍵Ｋｉを暗号化して保存を行うものとし、利用し終わった鍵は消去或いは破壊される場合もあるものとする。

【０１７２】また本実施形態では、実施形態２と同様にしてコンテンツ配送処理を行う。すなわち、図１３に示す様に情報提供端末１のコンテンツ暗号化部２１３は、鍵保存部２１２によって保存された鍵の内、鍵提供端末５の鍵更新部９１２により指定された識別情報ｉの暗号鍵Ｋｉを用いてコンテンツＣを暗号化し、前記暗号化されたコンテンツである暗号化コンテンツＫｉ（Ｃ）をコンテンツ配送部２１４によりマルチキャストで各情報利用端末に配送する処理を行う。

【０１７３】また図１４に示す様に各情報利用端末のコンテンツ取得部３１３は、暗号化コンテンツＫｉ（Ｃ）を情報提供端末１からマルチキャストで取得し、前記取得した暗号化コンテンツＫｉ（Ｃ）の暗号化で用いられた暗号鍵Ｋｉの識別情報ｉを識別情報確認部１０１１により確認する。そしてコンテンツ復号化部３１４は、鍵保存部３１２によって保存されていた鍵の内、識別情報確認部１０１１により指定された識別情報ｉの暗号鍵Ｋｉを用いて暗号化コンテンツＫｉ（Ｃ）を復号化し、前記復号化されたコンテンツＣをコンテンツ再生部３１５により再生する処理を行う。

【０１７４】前記の様に本実施形態の鍵提供端末５は、利用資格者ＤＢ２００８のデータを基に鍵を配送するため、脱退日時が経過したもの或いは次配送の鍵が脱退日時以降のコンテンツに該当する鍵である場合に情報利用端末への鍵の配送を取り止めることができる。

【０１７５】以上説明した様に本実施形態の情報配送システムによれば、コンテンツの利用資格を持つ利用者を示す配送先リストへの加入要求の受付が行われた利用者の情報利用端末に対して復号鍵を配送するので、利用者がコンテンツの利用資格を失っても復号する手段を保持し続けることが可能であると言う問題点を解決し、マルチキャストで配送するストリームコンテンツに対して、利用者の入れ替わりに対応できる利用制御を行うことが可能である。

【０１７６】（実施形態５）以下に利用者の加入及び脱退に応じてコンテンツの復号鍵の配送先を管理し、鍵更新広報により鍵提供端末の復号鍵を各情報利用端末から取得する実施形態５の情報配送システムについて説明する。

【０１７７】図２７は本実施形態の鍵提供端末５の概略構成を示す図である。図２７に示す様に本実施形態の鍵提供端末５は、加入要求応答部２７１１と、脱退要求応答部２７１２とを有している。

【０１７８】加入要求応答部２７１１は、コンテンツの利用資格を持つ利用者を示す配送先リストへの加入要求が受付けられたことを示す加入要求応答を、当該加入要求を送信した情報利用端末へ通知する処理部である。脱退要求応答部２７１２は、前記配送先リストからの脱退要求が受付けられたことを示す脱退要求応答を、当該脱退要求を送信した情報利用端末へ通知する処理部である。

【０１７９】鍵提供端末５を加入要求応答部２７１１及び脱退要求応答部２７１２として機能させる為のプログラムは、ＣＤ－ＲＯＭ等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行され

るものとする。なお前記プログラムを記録する記録媒体はＣＤ－ＲＯＭ以外の他の記録媒体でも良い。また前記プログラムを当該記録媒体から情報処理装置にインストールして使用しても良いし、ネットワークを通じて当該記録媒体にアクセスして前記プログラムを使用するものとしても良い。

【０１８０】本実施形態において、情報提供端末１と情報利用端末２～４と鍵提供端末５は、実施形態１と同様にそれぞれインターネットに接続されており、ネットワーク上でマルチキャストとユニキャストの通信が可能であるものとする。本実施形態では、ストリームコンテンツをマルチキャストで情報利用端末２～４に配送する情報提供端末１と、そのストリームコンテンツを暗号化または復号化する為の鍵を配送する鍵提供端末５とが別装置であるものとして説明するが、両者を同一の装置で実現しても良い。また本実施形態では鍵提供端末５で鍵を生成するものとするが、情報提供端末１で鍵を生成するものとしても良い。

【０１８１】なお本実施形態において、鍵提供端末５のその他の構成は実施形態３と同様であるものとし、情報提供端末１は利用資格者ＤＢ２００８が鍵提供端末５にあることを除いて実施形態１と同様の構成であるものとする。

【０１８２】図２８は本実施形態の情報利用端末２の概略構成を示す図である。図２８に示す様に本実施形態の情報利用端末２は、加入要求応答受付部２８１１と、脱退要求応答受付部２８１２とを有している。

【０１８３】加入要求応答受付部２８１１は、前記配送先リストへの加入要求が受付けられたことを示す加入要求応答を鍵提供端末５から受信する処理部である。脱退要求応答受付部２８１２は、前記配送先リストからの脱退要求が受付けられたことを示す脱退要求応答を鍵提供端末５から受信する処理部である。

【０１８４】情報利用端末２を加入要求応答受付部２８１１及び脱退要求応答受付部２８１２として機能させる為のプログラムは、ＣＤ－ＲＯＭ等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する記録媒体はＣＤ－ＲＯＭ以外の他の記録媒体でも良い。また前記プログラムを当該記録媒体から情報処理装置にインストールして使用しても良いし、ネットワークを通じて当該記録媒体にアクセスして前記プログラムを使用するものとしても良い。

【０１８５】本実施形態において、情報利用端末２のその他の構成は実施形態３と同様であるものとし、情報利用端末３及び４についても情報利用端末２の構成と同様であるものとする。

【０１８６】本実施形態の情報提供端末１には、配送対象のストリームコンテンツが保存されているか、或いはリアルタイムでストリームコンテンツが取得されるものとし、鍵提供端末５から情報提供端末１及び情報利用端末に鍵を、また情報提供端末１から各情報利用端末に暗号化コンテンツを送付し、各情報利用端末で暗号化コンテンツを復号化して再生する際の例について説明する。なおこの例ではコンテンツの暗号化に利用される暗号鍵は復号鍵を兼ねており、その鍵は所定の時間間隔で更新されるものとする。なお利用資格変更に伴って鍵が更新されるものとしたり、公開鍵暗号方式の様に暗号鍵と復号鍵とが異なるものとしても良く、暗号鍵と復号鍵とが異なるものとした場合には、情報提供端末１に暗号鍵を配送し、コンテンツの利用資格を持つ利用者の情報利用端末には復号鍵の配送を行うものとする。また更新の際は鍵提供端末５が呼びかけ、それに応じる形で情報利用端末２～４が鍵の更新を行なうものとする。

【０１８７】図２９は本実施形態の加入要求処理の処理手順を示すフローチャートである。図２９に示す様に各情報利用端末の加入要求部２１１１は、コンテンツの利用資格を持つ利用者を示す配送先リストへの加入要求を鍵提供端末５に送信する処理を行い、加入要求応答受付部２８１１は、前記配送先リストへの加入要求が受付けられたことを示す加入要求応答を鍵提供端末５から受信する処理を行う。

【０１８８】ステップ２９０１で各情報利用端末の加入要求部２１１１は、コンテンツの利用資格を持つ利用者を示す配送先リストへの加入指示の利用者からの入力を受付けているかどうかを調べ、前記配送先リストへの加入指示を受付けている場合にはステップ２９０２へ進む。

【０１８９】ステップ２９０２では、当該情報利用端末を一意に指定できる情報として、情報利用端末の識別子、ＩＰアドレス、サービス加入時のユーザ情報または端末情報等を磁気ディスク装置３０３から読み出す。

【０１９０】ステップ２９０３では、利用者が加入したいチャネル情報として、コンテンツの名称、コンテンツ識別情報、マルチキャストアドレス等の情報と、当該コンテンツの利用を開始したい日時を示す加入日時の入力を受付ける。ここで当該コンテンツの利用可能な期間を示す加入期間や、当該コンテンツの利用を終了したい日時を示す脱退日時の入力を受付けても良い。また加入日時を省略しても構わないものとし、省略可能とする場合は省略時の加入日時は「即時」であるとする等予め規則を決めておくものとする。

【０１９１】ステップ２９０４では、前記読み出した当該情報利用端末を一意に指定できる情報及び前記受付けたチャネル情報と共に、前記配送先リストへの加入要求を鍵提供端末５に送信する。

【０１９２】ステップ２９０５で加入要求応答受付部２８１１は、前記配送先リストからの加入要求が受付けられたことを示す加入要求応答を鍵提供端末５から受信しているかどうかを調べ、前記加入要求応答を受信してい

る場合にはステップ２９０６へ進む。ステップ２９０６では、前記受信した加入要求応答の内容を出力装置３０５へ表示して加入要求の結果を利用者へ知らせる。

【０１９３】図３０は本実施形態の加入要求受付処理の処理手順を示すフローチャートである。図３０に示す様に鍵提供端末５の加入要求受付部２０１１は、前記配送先リストへの加入要求を情報利用端末２～４から受付ける処理を行い、加入要求応答部２７１１は、前記配送先リストへの加入要求が受付けられたことを示す加入要求応答を、当該加入要求を送信した情報利用端末へ通知する処理を行う。

【０１９４】ステップ３００１で鍵提供端末５の加入要求受付部２０１１は、コンテンツの利用資格を持つ利用者を示す配送先リストへの加入要求と情報利用端末を一意に指定できる情報及びチャネル情報を情報利用端末２～４から受信しているかどうかを調べ、前記配送先リストへの加入要求を受信している場合にはステップ３００２へ進む。

【０１９５】ステップ３００２でデータベース部２０１２は、前記加入要求と共に送信された、情報利用端末の識別子、ＩＰアドレス、サービス加入時のユーザ情報または端末情報等の情報利用端末を一意に指定できる情報や、コンテンツの名称、コンテンツ識別情報、マルチキャストアドレス等のチャネル情報、当該コンテンツの利用を開始したい日時を示す加入日時を利用資格者ＤＢ２００８に格納する。ここで当該コンテンツの利用可能な期間を示す加入期間や、当該コンテンツの利用を終了したい日時を示す脱退日時も送信されている場合には、脱退日時の格納も行う。また加入日時が省略されている場合には、予め決められている規則に従って加入日時を「即時」等に設定する。

【０１９６】ステップ３００３で加入要求応答部２７１１は、前記配送先リストへの加入要求が受付けられたことを示す加入要求応答を、当該加入要求を送信した情報利用端末へ通知する処理を行う。

【０１９７】図３１は本実施形態の脱退要求処理の処理手順を示すフローチャートである。図３１に示す様に各情報利用端末の脱退要求部２１１２は、前記配送先リストからの脱退要求を鍵提供端末５に送信する処理を行い、脱退要求応答受付部２８１２は、前記配送先リストからの脱退要求が受付けられたことを示す脱退要求応答を鍵提供端末５から受信する処理を行う。なお加入要求時に加入期間や脱退日時の入力を行っている場合にはこの脱退要求処理を省略することができる。

【０１９８】ステップ３１０１で各情報利用端末の脱退要求部２１１２は、コンテンツの利用資格を持つ利用者を示す配送先リストからの脱退指示の利用者からの入力を受付けているかどうかを調べ、前記配送先リストからの脱退指示を受付けている場合にはステップ３１０２へ進む。

【０１９９】ステップ３１０２では、当該情報利用端末を一意に指定できる情報として、情報利用端末の識別子、ＩＰアドレス、サービス脱退時のユーザ情報または端末情報等を磁気ディスク装置３０３から読み出す。

【０２００】ステップ３１０３では、利用者が脱退したいチャネル情報として、コンテンツの名称、コンテンツ識別情報、マルチキャストアドレス等の情報と、当該コンテンツの利用を終了したい日時を示す脱退日時の入力を受付ける。ここで脱退日時を省略しても構わないものとし、省略可能とする場合は省略時の脱退日時は「即時」であるとする等予め規則を決めておくものとする。

【０２０１】ステップ３１０４では、前記読み出した当該情報利用端末を一意に指定できる情報及び前記受付けたチャネル情報と共に、前記配送先リストからの脱退要求を鍵提供端末５に送信する。

【０２０２】ステップ３１０５で脱退要求応答受付部２８１２は、前記配送先リストからの脱退要求が受付けられたことを示す脱退要求応答を鍵提供端末５から受信しているかどうかを調べ、前記脱退要求応答を受信している場合にはステップ３１０６へ進む。ステップ３１０６では、前記受信した脱退要求応答の内容を出力装置３０５へ表示して脱退要求の結果を利用者へ知らせる。

【０２０３】図３２は本実施形態の脱退要求受付処理の処理手順を示すフローチャートである。図３２に示す様に鍵提供端末５の脱退要求受付部２０１３は、前記配送先リストからの脱退要求を情報利用端末２～４から受付ける処理を行い、脱退要求応答部２７１２は、前記配送先リストからの脱退要求が受付けられたことを示す脱退要求応答を、当該脱退要求を送信した情報利用端末へ通知する処理を行う。

【０２０４】ステップ３２０１で鍵提供端末５の脱退要求受付部２０１３は、コンテンツの利用資格を持つ利用者を示す配送先リストからの脱退要求と情報利用端末を一意に指定できる情報及びチャネル情報を情報利用端末２～４から受信しているかどうかを調べ、前記配送先リストへの脱退要求を受信している場合にはステップ３２０２へ進む。

【０２０５】ステップ３２０２でデータベース部２０１２は、前記脱退要求と共に送信された情報利用端末を一意に指定できる情報及びチャネル情報に該当するレコードを利用資格者ＤＢ２００８から検索し、前記チャネル情報中の脱退日時の情報を当該レコードに格納する。また脱退日時が省略されている場合には、予め決められている規則に従って脱退日時を「即時」等に設定する。

【０２０６】ステップ３２０３で脱退要求応答部２７１２は、前記配送先リストからの脱退要求が受付けられたことを示す脱退要求応答を、当該脱退要求を送信した情報利用端末へ通知する処理を行う。

【０２０７】図３３は本実施形態の鍵提供端末５の鍵配送処理の処理手順を示すフローチャートである。図３３

に示す様に鍵提供端末５では、ストリームコンテンツであるコンテンツＣを暗号化または復号化する為の暗号鍵Ｋｉを生成した後、鍵更新広報部１５１１により新規の暗号鍵Ｋｉの取得を促す鍵更新広報をマルチキャストで各情報利用端末に送信し、各情報利用端末からの接続を受付けてその暗号鍵Ｋｉをユニキャストで配送する処理を行う。

【０２０８】図３３のステップ３３０１で鍵提供端末５の鍵生成部４１１は、所定の時間が経過した場合や情報提供端末１の利用資格者ＤＢ２００８中の利用資格が変更された場合等の暗号鍵Ｋを生成する条件が成立したかどうかを調べ、暗号鍵Ｋを生成する条件が成立した場合にはステップ３３０２へ進む。

【０２０９】ステップ３３０２では、コンテンツＣを暗号化する為の暗号鍵Ｋを生成する。暗号鍵Ｋとして通信時にＩＰｓｅｃで利用されているものを利用しても構わないものとする。

【０２１０】ステップ３３０３で識別情報付加部９１１は、前記生成された暗号鍵Ｋに識別情報ｉを付加して鍵配送部４１２へ渡す。この識別情報はＩＰｓｅｃのＳＡに含まれる情報を利用しても構わないものとする。

【０２１１】ステップ３３０４で鍵配送部４１２は、前記生成された暗号鍵Ｋｉをユニキャストで情報提供端末１へ配送する。ここで配送の際にＩＰｓｅｃ等を用いて通信路をセキュアな状態に保っても構わないものとする。

【０２１２】ステップ３３０５で鍵更新広報部１５１１は、各情報利用端末に向けて新規の暗号鍵Ｋｉの取得を促す鍵更新広報をマルチキャストにより送信する。ここで利用資格者ＤＢ２００８を検索して鍵の配送の対象となる利用者を特定し、その利用者の情報利用端末に対してユニキャストで鍵更新広報を通知しても構わないものとする。この広報を受け取った各情報利用端末は、暗号鍵Ｋｉを取得する為に鍵提供端末５へユニキャストで接続する。

【０２１３】ステップ３３０６で鍵配送部４１２は、ユニキャストを用いた情報利用端末からの接続要求があるかどうかを調べ、情報利用端末からの接続要求がある場合にはステップ３３０７へ進む。

【０２１４】ステップ３３０７では、情報提供端末１の利用資格者ＤＢ２００８の内容を参照し、前記接続要求を送信した利用者のレコードの加入日時及び脱退日時を読み出す。

【０２１５】ステップ３３０８では、現在の日時と利用資格者ＤＢ２００８から前記読み出した加入日時とを比較し、それらの差が所定の時間以内であるかまたは現在の日時が前記加入日時を経過している場合にはステップ３３０９へ進む。

【０２１６】ステップ３３０９では、現在の日時と利用資格者ＤＢ２００８から前記読み出した脱退日時とを比較し、現在の日時が前記脱退日時を経過しておらず、配送対象の鍵が脱退日時以前に配送されるコンテンツの鍵である場合にはステップ３３１０へ進む。

【０２１７】ステップ３３１０では、前記レコードから前記接続要求を行った情報利用端末のＩＰアドレスを読み出し、そのＩＰアドレスを宛先としたユニキャストによって暗号鍵Ｋｉを配送する。ここで配送の際にＩＰｓｅｃ等を用いて通信路をセキュアな状態に保っても構わないものとする。

【０２１８】ステップ３３１１では、前記利用資格を持つ全ての利用者の情報利用端末に暗号鍵Ｋｉを配送したかどうかを調べ、まだ配送を行っていない情報利用端末がある場合にはステップ３３０６へ戻って他の情報利用端末からの接続要求を待ち、利用資格を持つ全ての利用者の情報利用端末への配送を完了した場合にはステップ３３１２へ進む。ここで鍵の配送の完了とは、各情報利用端末と鍵提供端末５がユニキャストで鍵の通信を行って正常終了した場合の他に、情報利用端末２～４からの応答が無く、タイムアウトした場合を含んでいても構わないものとする。また鍵提供端末５の鍵配送に対する応答を所定時間で区切り、その区切りをもって鍵配送完了通知としても構わないものとする。

【０２１９】ステップ３３１２では、利用資格を持った全ての利用者に対する暗号鍵Ｋｉの配送が完了したことを示す鍵配送完了通知を鍵更新部９１２に伝え、ステップ３３１３で鍵更新部９１２は、配送が完了した暗号鍵Ｋｉを次の暗号化処理で使用する鍵として決定し、その暗号鍵Ｋｉの識別情報ｉ或いは暗号鍵Ｋｉそのものの情報を情報提供端末１のコンテンツ暗号化部２１３に通知してステップ３３０１へ戻る。

【０２２０】次に本実施形態の情報利用端末２～４では、実施形態３と同様にして暗号鍵Ｋｉを取得する。すなわち図１８に示す様に各情報利用端末の鍵更新情報取得部１６１１は、鍵提供端末５からマルチキャストで新規の暗号鍵Ｋｉの取得を促す鍵更新広報を受信して鍵提供端末５へユニキャストで接続し、鍵提供端末５からユニキャストで暗号鍵Ｋｉを受信して鍵保存部３１２に渡す。そして鍵保存部３１２は、鍵提供端末５の識別情報付加部９１１によって付加された識別情報ｉ毎に暗号鍵Ｋｉを分類してメモリ３０２または磁気ディスク装置３０３に保存する。ここで磁気ディスク装置３０３に保存する場合には暗号鍵Ｋｉを暗号化して保存を行うものとし、利用し終わった鍵は消去或いは破壊される場合もあるものとする。

【０２２１】また本実施形態では、実施形態２と同様にしてコンテンツ配送処理を行う。すなわち、図１３に示す様に情報提供端末１のコンテンツ暗号化部２１３は、鍵保存部２１２によって保存された鍵の内、鍵提供端末５の鍵更新部９１２により指定された識別情報ｉの暗号鍵Ｋｉを用いてコンテンツＣを暗号化し、前記暗号化さ

れたコンテンツである暗号化コンテンツＫｉ（Ｃ）をコンテンツ配送部２１４によりマルチキャストで各情報利用端末に配送する処理を行う。

【０２２２】また図１４に示す様に各情報利用端末のコンテンツ取得部３１３は、暗号化コンテンツＫｉ（Ｃ）を情報提供端末１からマルチキャストで取得し、前記取得した暗号化コンテンツＫｉ（Ｃ）の暗号化で用いられた暗号鍵Ｋｉの識別情報ｉを識別情報確認部１０１１により確認する。そしてコンテンツ復号化部３１４は、鍵保存部３１２によって保存されていた鍵の内、識別情報確認部１０１１により指定された識別情報ｉの暗号鍵Ｋｉを用いて暗号化コンテンツＫｉ（Ｃ）を復号化し、前記復号化されたコンテンツＣをコンテンツ再生部３１５により再生する処理を行う。

【０２２３】前記の様に本実施形態の鍵提供端末５は、利用資格者ＤＢ２００８のデータを基に鍵を配送するため、鍵提供端末５からの鍵更新広報に対して情報利用端末から鍵の取得要求が行われた場合でも、脱退日時が経過したり、或いは次配送の鍵が脱退日時以降のコンテンツの鍵である場合に当該情報利用端末への鍵の配送を取り止めることができる。

【０２２４】以上説明した様に本実施形態の情報配送システムによれば、コンテンツの利用資格を持つ利用者を示す配送先リストへの加入要求の受付が行われた利用者の情報利用端末に対して復号鍵を配送するので、利用者がコンテンツの利用資格を失っても復号する手段を保持し続けることが可能であると言う問題点を解決し、マルチキャストで配送するストリームコンテンツに対して、利用者の入れ替わりに対応できる利用制御を行うことが可能である。

【０２２５】

【発明の効果】本発明によればマルチキャストで情報提供端末から各情報利用端末に配送された暗号化コンテンツを、ユニキャストで当該情報利用端末に配送された鍵によって復号化するので、利用者がコンテンツの利用資格を失っても復号化する手段を保持し続けることが可能であると言う従来の問題点を解決し、マルチキャストで配送されるコンテンツに対して、利用者の入れ替わりに対応した利用制御を行うことが可能である。

【図面の簡単な説明】

【図１】実施形態１の情報配送システムの概略構成を示す図である。

【図２】実施形態１の情報提供端末１の概略構成を示す図である。

【図３】実施形態１の情報利用端末２の概略構成を示す図である。

【図４】実施形態１の鍵提供端末５の概略構成を示す図である。

【図５】実施形態１の鍵提供端末５の鍵配送処理の処理手順を示すフローチャートである。

【図６】実施形態１の情報提供端末１または各情報利用端末の鍵取得処理の処理手順を示すフローチャートである。

【図７】実施形態１の情報提供端末１のコンテンツ配送処理の処理手順を示すフローチャートである。

【図８】実施形態１の各情報利用端末のコンテンツ利用処理の処理手順を示すフローチャートである。

【図９】実施形態２の鍵提供端末５の概略構成を示す図である。

【図１０】実施形態２の情報利用端末２の概略構成を示す図である。

【図１１】実施形態２の鍵提供端末５の鍵配送処理の処理手順を示すフローチャートである。

【図１２】実施形態２の情報提供端末１または各情報利用端末の鍵取得処理の処理手順を示すフローチャートである。

【図１３】実施形態２の情報提供端末１のコンテンツ配送処理の処理手順を示すフローチャートである。

【図１４】実施形態２の各情報利用端末のコンテンツ利用処理の処理手順を示すフローチャートである。

【図１５】実施形態３の鍵提供端末５の概略構成を示す図である。

【図１６】実施形態３の情報利用端末２の概略構成を示す図である。

【図１７】実施形態３の鍵提供端末５の鍵配送処理の処理手順を示すフローチャートである。

【図１８】実施形態３の情報提供端末１または各情報利用端末の鍵取得処理の処理手順を示すフローチャートである。

【図１９】実施形態４の情報配送システムの概略構成を示す図である。

【図２０】実施形態４の鍵提供端末５の概略構成を示す図である。

【図２１】実施形態４の情報利用端末２の概略構成を示す図である。

【図２２】実施形態４の加入要求処理の処理手順を示すフローチャートである。

【図２３】実施形態４の加入要求受付処理の処理手順を示すフローチャートである。

【図２４】実施形態４の脱退要求処理の処理手順を示すフローチャートである。

【図２５】実施形態４の脱退要求受付処理の処理手順を示すフローチャートである。

【図２６】実施形態４の鍵提供端末５の鍵配送処理の処理手順を示すフローチャートである。

【図２７】実施形態５の鍵提供端末５の概略構成を示す図である。

【図２８】実施形態５の情報利用端末２の概略構成を示す図である。

【図２９】実施形態５の加入要求処理の処理手順を示す

フローチャートである。

【図３０】実施形態５の加入要求受付処理の処理手順を示すフローチャートである。

【図３１】実施形態５の脱退要求処理の処理手順を示すフローチャートである。

【図３２】実施形態５の脱退要求受付処理の処理手順を示すフローチャートである。

【図３３】実施形態５の鍵提供端末５の鍵配送処理の処理手順を示すフローチャートである。

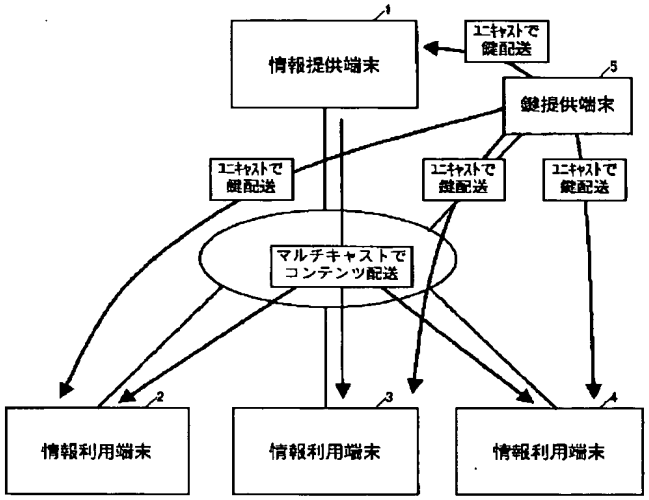
【符号の説明】

１…情報提供端末、２～４…情報利用端末、５…鍵提供端末、２０１…ＣＰＵ、２０２…メモリ、２０３…磁気ディスク装置、２０４…入力装置、２０５…出力装置、２０６…ＣＤ－ＲＯＭ装置、２０７…通信装置、２１１…鍵取得部、２１２…鍵保存部、２１３…コンテンツ暗号化部、２１４…コンテンツ配送部、３０１…ＣＰＵ、

３０２…メモリ、３０３…磁気ディスク装置、３０４…入力装置、３０５…出力装置、３０６…ＣＤ－ＲＯＭ装置、３０７…通信装置、３１１…鍵取得部、３１２…鍵保存部、３１３…コンテンツ取得部、３１４…コンテンツ復号化部、３１５…コンテンツ再生部、４０１…ＣＰＵ、４０２…メモリ、４０３…磁気ディスク装置、４０４…入力装置、４０５…出力装置、４０６…ＣＤ－ＲＯＭ装置、４０７…通信装置、４１１…鍵生成部、４１２…鍵配送部、９１１…識別情報付加部、９１２…鍵更新部、１０１１…識別情報確認部、１５１１…鍵更新広報部、１６１１…鍵更新情報取得部、２００８…利用資格者ＤＢ、２０１１…加入要求受付部、２０１２…データベース部、２０１３…脱退要求受付部、２１１１…加入要求部、２１１２…脱退要求部、２７１１…加入要求応答部、２７１２…脱退要求応答部、２８１１…加入要求応答受付部、２８１２…脱退要求応答受付部。

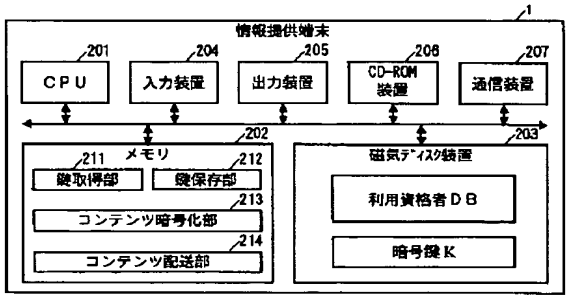
【図１】

図１



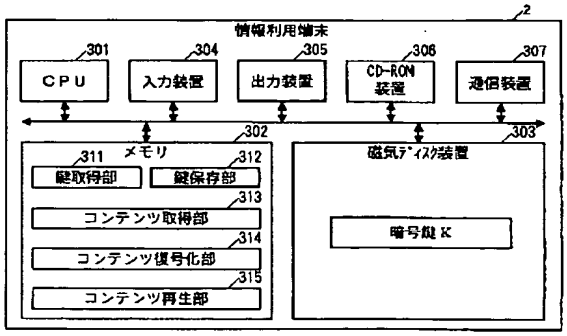
【図２】

図２



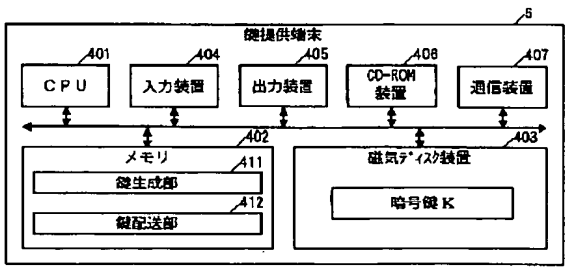
【図３】

図３



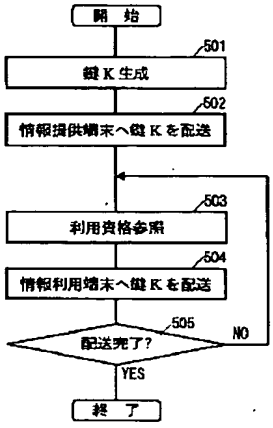
【図４】

図４



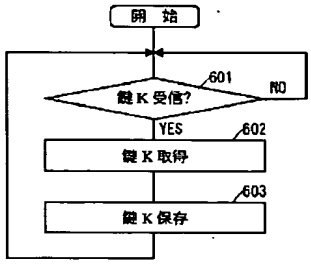
【図５】

図５



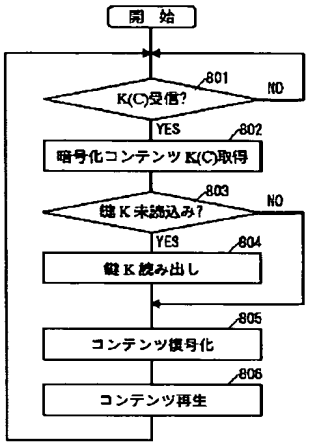
【図６】

図６



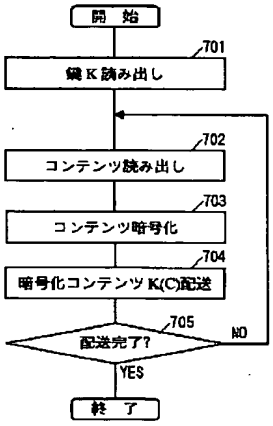
【図８】

図８



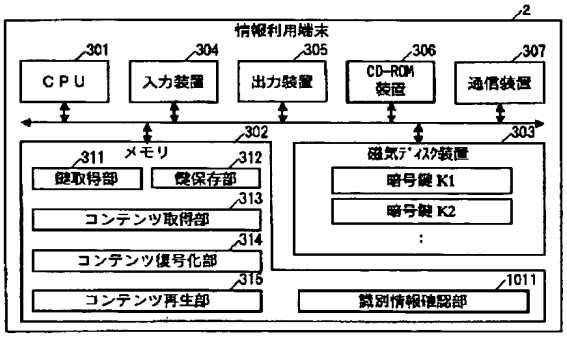
【図７】

図７



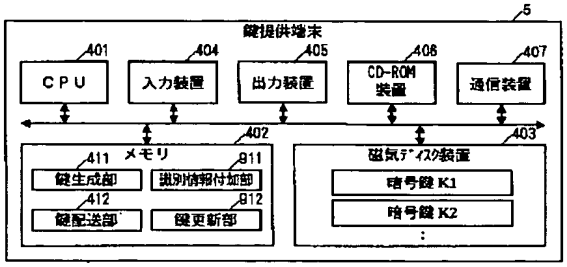
【図１０】

図１０



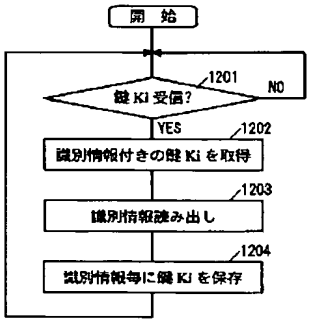
【図９】

図９



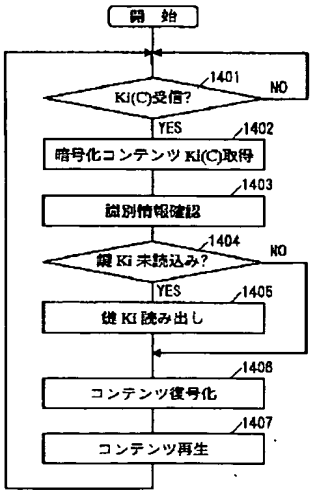
【図１２】

図１２



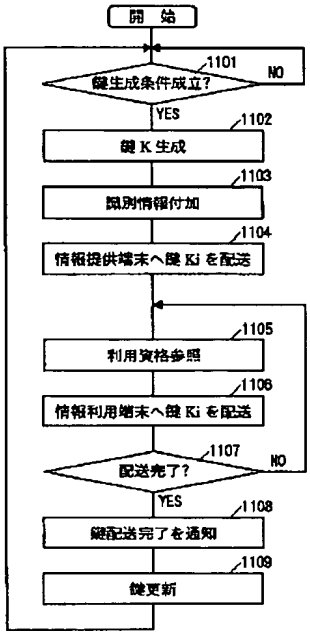
【図１４】

図１４



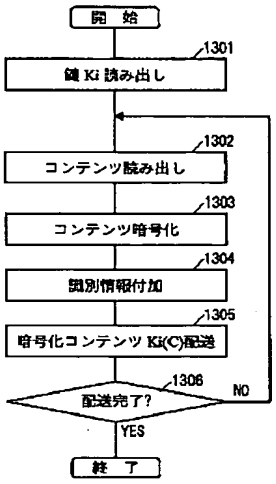
【図１１】

図１１



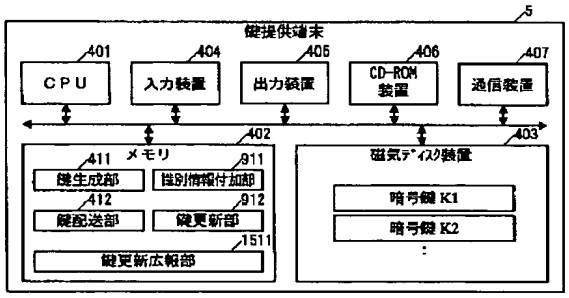
【図１３】

図１３



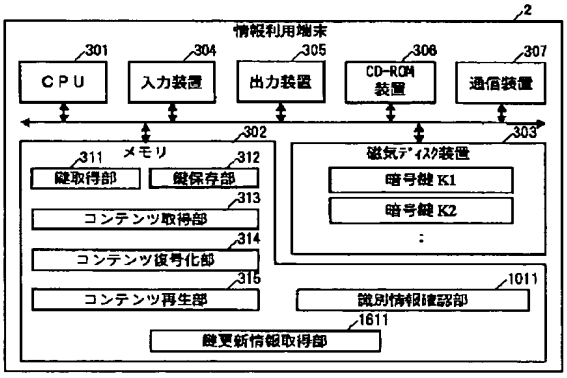
【図１５】

図１５



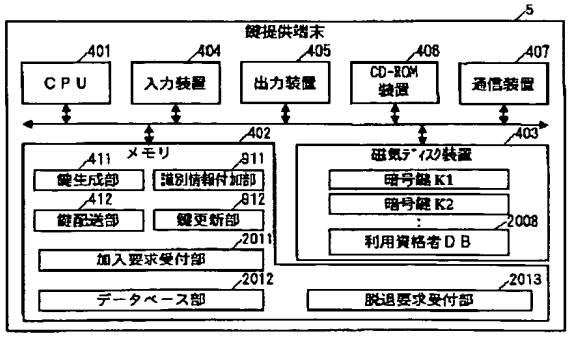
【図１６】

図１６



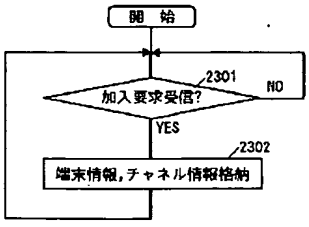
【図２０】

図２０



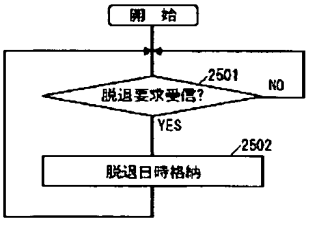
【図２３】

図２３



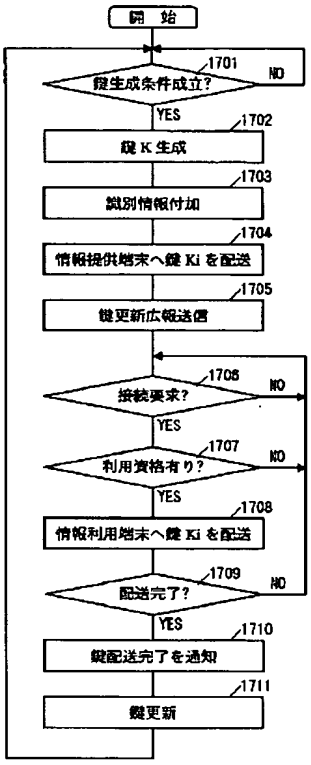
【図２５】

図２５



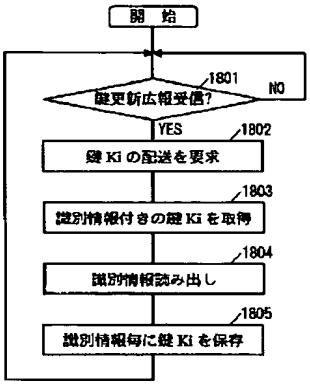
【図１７】

図１７



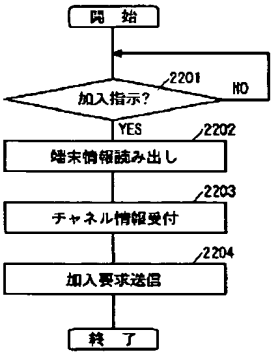
【図１８】

図１８



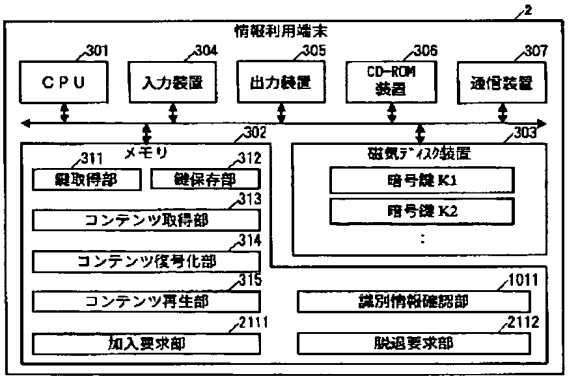
【図２２】

図２２



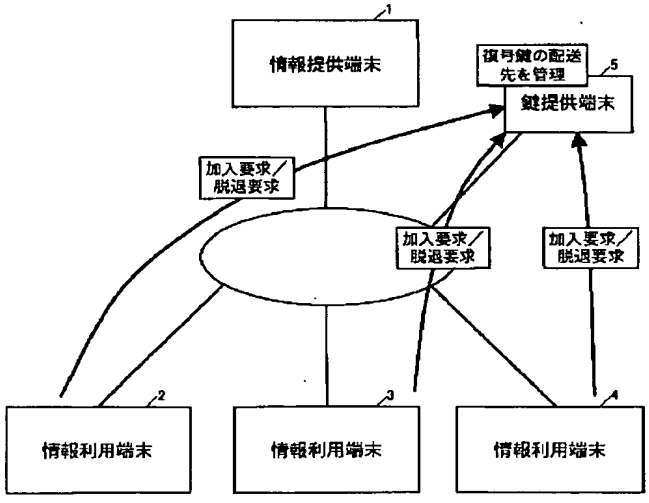
【図２１】

図２１



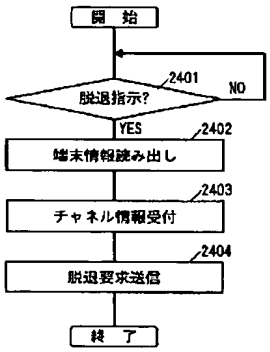
【図１９】

図１９



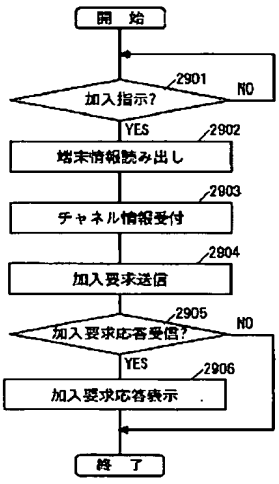
【図２４】

図２４



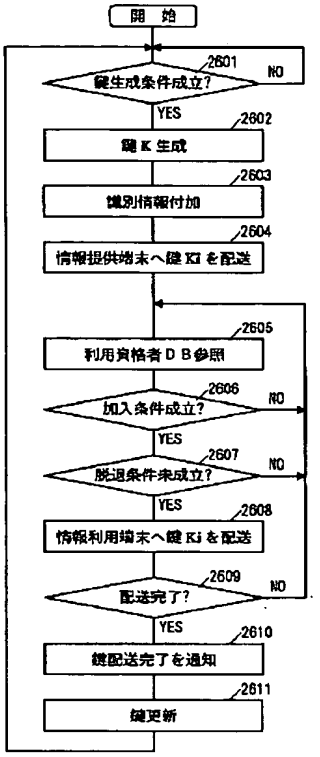
【図２９】

図２９



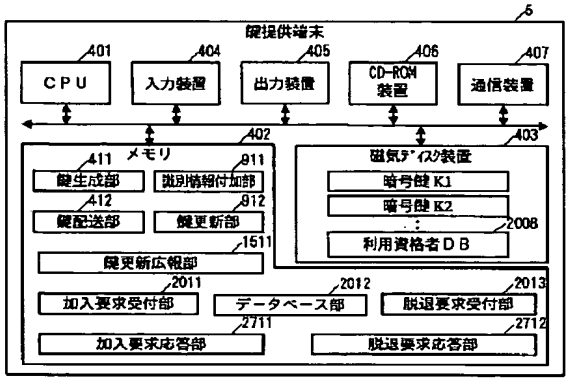
【図２６】

図２６



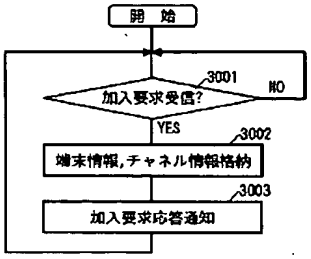
【図２７】

図２７



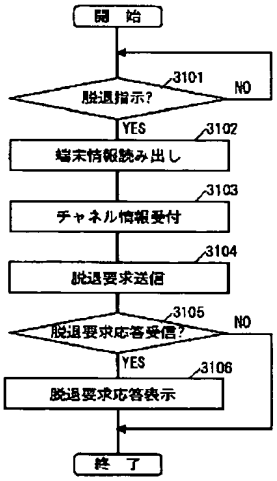
【図３０】

図３０



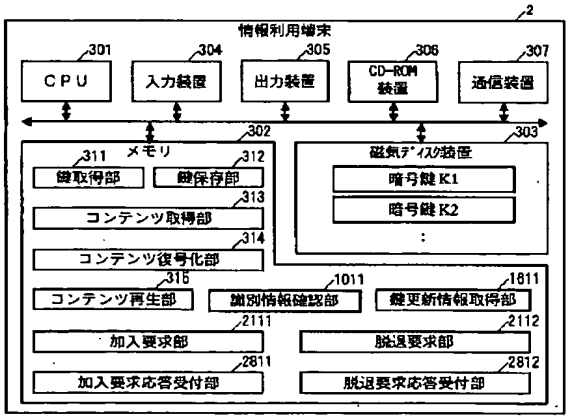
【図３１】

図３１



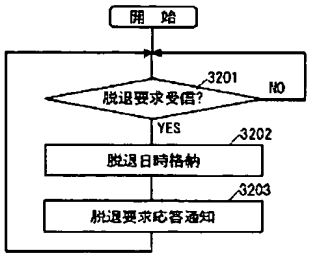
【図２８】

図２８



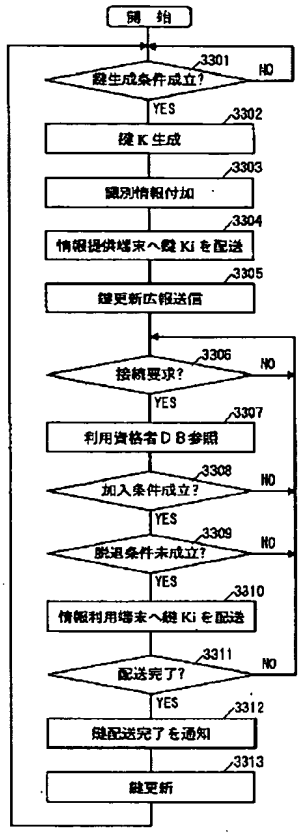
【図３２】

図３２



【図３３】

図３３



フロントページの続き

Ｆターム(参考) 5B085 AE13 BG07 CA04
5J104 AA12 AA16 EA04 EA16 EA21
NA02 PA07
5K030 GA15 HA08 HC01 LD06 LD19